



Republika Hrvatska
Agencija za zaštitu osobnih podataka

MIŠLJENJA, PRIMJERI I PREPORUKE

AGENCIJE ZA ZAŠTITU OSOBNIH PODATAKA

PRILOG

GODIŠNJEM IZVJEŠĆU O RADU

AGENCIJE ZA ZAŠTITU OSOBNIH PODATAKA

za razdoblje od 1. siječnja 2018. do 31. prosinca 2018.

| ožujak, 2019.

I PRIMJERI STRUČNIH MIŠLJENJA – NEUPRAVNI POSTUPAK	3
- POSTUPANJE PO ZAPRIMLJENIM UPITIMA PRAVNIH OSOBA, JAVNOPRAVNIH TIJELA I GRAĐANA.....	3
DAVANJE STRUČNIH MIŠLJENJA	3
- <i>Stručna mišljenja, izdana na zahtjev građana</i>	3
- <i>Stručna mišljenja izdana na zahtjev tijela javne vlasti</i>	3
- <i>Značajni primjeri iz prakse.....</i>	3
I PRIMJERI STRUČNIH MIŠLJENJA IZ PRAKSE	4
<i>Mišljenje 1 – potpis za raspisivanje referenduma Građanskih inicijativa</i>	4
<i>Mišljenje 2 – iskazivanje dijagnoze na liječničkom nalazu</i>	5
<i>Mišljenje 3 – objava osobnih podataka djece na web stranici trgovačkog centra.....</i>	5
<i>Mišljenje 4 – obrada osobnih podataka koju provode agencije za naplatu potraživanja</i>	6
<i>Mišljenje 5 – prijenos osobnih podataka zaposlenika tijela javne vlasti u drugu državu članicu Europske unije</i>	9
<i>Mišljenje 6 – prijenos osobnih podataka zaposlenika u treće zemlje koje nisu članice EU</i>	11
<i>Mišljenje 7 – prijenos registarskih oznaka u druge države članice EU</i>	13
I PREPORUKE, SAVJETI I MIŠLJENJA ZA UNAPRJEĐIVANJE ZAŠTITE OSOBNIH PODATAKA DANI UNUTAR NADZORNIH AKTIVNOSTI AGENCIJE	14
I KARAKTERISTIČNI SLUČAJEVI IZ NADZORNE PRAKSE PROVOĐENJA ZAŠTITE OSOBNIH PODATAKA	17
NADZOR U SEKTORU TIJELA JAVNE VLASTI KOD VODITELJA ZBIRKI OSOBNIH PODATAKA: MINISTARSTVO FINANCIJA/POREZNA UPRAVA, ZAGREB, TE NADZOR U SEKTORU GOSPODARSTVA, KOD VODITELJA ZBIRKI OSOBNIH PODATAKA: FINA – FINANCIJSKA AGENCIJA, ZAGREB.	17
NADZOR U SEKTORU TIJELA JAVNE VLASTI KOD VODITELJA ZBIRKI OSOBNIH PODATAKA: MINISTARSTVO UPRAVE, ZAGREB.	19
NADZOR U SEKTORU TIJELA JAVNE VLASTI KOD VODITELJA ZBIRKI OSOBNIH PODATAKA: MINISTARSTVO UNUTARNJIH POSLOVA, ZAGREB, TE NADZOR U SEKTORU TIJELA JAVNE VLASTI, KOD VODITELJA ZBIRKI OSOBNIH PODATAKA: MINISTARSTVO FINANCIJA/POREZNA UPRAVA, ZAGREB.	20
AGENCIJI SE OBRATILA PRAVNA OSOBA SA PITANJEM SMIJU LI VLASNICI TRGOVAČKIH DRUŠTAVA SA SJEDIŠTEM U REPUBLICI HRVATSKOJ IZNOSITI DOKUMENTACIJU ISTIH NAKON NJIHOVE LIKVIDACIJE IZVAN REPUBLIKE HRVATSKE ILI SE ONA FIZIČKI MORA ČUVATI ISKLJUČIVO U REPUBLICI HRVATSKOJ. AGENCIJA SE OČITOVALA KAKO SLIJEDI:.....	21
AGENCIJI SE OBRATILA ODVJETNICA IZ ZAGREBA SA PITANJEM ŠTO SVE TREBA DOSTAVITI AGENCIJI DA SE DOBIJE SUGLASNOST ZA IZNOŠENJE OSOBNIH PODATAKA U TREĆE ZEMLJE (KONKRETNO REPUBLIKU SRBIJU), KAKO IZGLEDA POSTUPAK I KOLIKO TRAJE. AGENCIJA SE OČITOVALA KAKO SLIJEDI:	24
AGENCIJI SE OBRATILO ODVJETNIČKO DRUŠTVO IZ REPUBLIKE HRVATSKE SA UPITOM MOŽE LI IZVRŠITELJ OBRADE KOJI IMA POSLOVNI NASTAN U REPUBLICI HRVATSKOJ ISTOVREMENO BITI IMENOVAN PREDSTAVNIKOM VODITELJA OBRADE ČIJI SE POSLOVNI NASTAN NALAZI IZVAN EUROSKE UNIJE. AGENCIJA SE OČITOVALA KAKO SLIJEDI:.....	27
AGENCIJI SE OBRATILA PRAVNA OSOBA SA SJEDIŠTEM U REPUBLICI SRBIJI SA UPITOM DA LI SE NA NJIH PRIMJENJUJE ODREDBA OPĆE UREDBE O IMENOVANJU PREDSTAVNIKA BUDUĆI DA IMAJU NAMJERU SVOJE POSLOVANJE PROŠIRITI NA REPUBLIKU HRVATSKU. AGENCIJA SE OČITOVALA KAKO SLIJEDI:	29
ODVJETNICA IZ ZAGREBA SE OBRATILA AGENCIJI U IME SVOJEG KLIJENTA – PRAVNE OSOBE SA SJEDIŠTEM U REPUBLICI HRVATSKOJ, SA UPITOM O PRAVNOJ TEMELJU ZA SLANJE ŽIVOTOPISA SVOJIH ZAPOSLENIKA POTENCIJALNIM KLIJENTIMA NA PODRUČJU REPUBLIKE HRVATSKE, ALI I IZVAN PODRUČJA REPUBLIKE HRVATSKE. AGENCIJA SE OČITOVALA KAKO SLIJEDI:	31
I POSTUPANJE PO PRITUŽBAMA / ZAHTJEVIMA ZA UTVRĐIVANJE	34
<i>POVREDE PRAVA - Provođenje upravnog postupka.....</i>	34
I PRIKAZ NEKOLIKO PRIMJERA IZ PRAKSE.....	34
<i>Primjer 1. – Objava osobnih podataka na Facebook profilu</i>	34
<i>Primjer 2. – Neovlašteno raspolaganje osobnim podacima.....</i>	35
<i>Primjer 3. – Objava osobnih podataka o zdravlju</i>	36
<i>Primjer 4. – Pravo uvida u osobne podatke.....</i>	36

<i>Primjer 5. – Postavljanje videonadzornih kamera u stambenim zgradama.....</i>	<i>37</i>
<i>Primjer 6. - Zloupotreba identiteta u telekomunikacijskom sektoru</i>	<i>37</i>
<i>Primjer 7. - Obrada osobnih podataka od strane agencija za naplatu potraživanja</i>	<i>38</i>
<i>Primjer 8. – Objava osobnih podataka po Zakonu o pravu na pristup informacijama</i>	<i>39</i>
I PROVOĐENJE POSTUPKA PO SLUŽBENOJ DUŽNOSTI	39
<i>Primjer 1. – Objava podataka u klasičnim (tiskanom izdanju) i digitalnim medijima</i>	<i>39</i>
<i>Primjer 2. – Videonadzor u školskoj ustanovi.....</i>	<i>40</i>
I UPRAVNI SPOROVI U 2018.	41
<i>Primjer 1. – Objava osobnih podataka u medijima</i>	<i>41</i>
<i>Primjer 2. – Objava osobnih podataka u medijima</i>	<i>42</i>
<i>Primjer 3. Obrada osobnih podataka videonadzorom</i>	<i>42</i>
<i>Primjer 4. – Obrada osobnih podataka videonadzorom u zajedničkim prostorijama suvlasnika</i>	<i>42</i>
<i>Primjer 5. – Prosljeđivanje osobnih podataka radnika drugim primateljima.....</i>	<i>43</i>
<i>Primjer 6. – Pravo pristupa/uvida u osobne podatke.....</i>	<i>43</i>
<i>Primjer 8. – Obradivanje osobnih podataka u svrhu sklapanja pretplatničkog ugovora</i>	<i>43</i>
<i>Primjer 9. – Obrada biometrijskih osobnih podataka</i>	<i>43</i>
<i>Primjer 10. – Neovlašten uvid i daljnje korištenje osobnih podataka</i>	<i>44</i>
I PREPORUKE ZA UNAPREĐENJE ZAŠTITE OSOBNIH PODATAKA.....	44
<i>Preporuka 1.....</i>	<i>44</i>
<i>Dostavljanje osobnih podataka/medicinskih nalaza elektroničkom poštom</i>	<i>44</i>
<i>Preporuka 2.....</i>	<i>45</i>
<i>Objava osobnih podataka kandidata u natječajnim postupcima</i>	<i>45</i>
<i>Preporuka 3. Korištenje bankovne kartice u svrhu beskontaktnog plaćanja</i>	<i>45</i>

PRIMJERI STRUČNIH MIŠLJENJA – Neupravni postupak

- **Postupanje po zaprimljenim upitima pravnih osoba, javnopravnih tijela i građana davanje stručnih mišljenja**
- **Stručna mišljenja, izdana na zahtjev građana**
- **Stručna mišljenja izdana na zahtjev tijela javne vlasti**
- **Značajni primjeri iz prakse**

PRIMJERI STRUČNIH MIŠLJENJA IZ PRAKSE

Mišljenje 1 – potpis za raspisivanje referenduma Građanskih inicijativa

Agenciji je zaprimila upit vezano uz preispitivanje zakonitosti ustupanja osobnih podataka građana koji su dali svoj potpis za raspisivanje referenduma Građanskih inicijativa te njihove obrade od strane Ministarstva uprave i društva APIS IT d.o.o. kao i činjenice da li je za takvu daljnju obradu osobnih podataka potrebna privola.

Agencija je dala mišljenje uzimajući u obzir odredbe Zakona o referendumu i drugim oblicima osobnog sudjelovanja u obavljanju državne vlasti i lokalne i područne (regionalne) samouprave („Narodne novine“ broj 33/96, 92/01, 44/06, 58/06, 69/07, 38/09, 100/16, 73/17) (dalje u tekstu Zakon o referendumu), koji u članku 3. propisuje kako Hrvatski sabor može raspisati referendum o prijedlogu za promjenu Ustava, o prijedlogu zakona ili o drugom pitanju iz svojeg djelokruga. Hrvatski sabor će raspisati referendum o ovim pitanjima ako to zatraži deset posto od ukupnog broja birača u Republici Hrvatskoj. S time u vezi, imajući u vidu odredbe članka 3. Zakona o referendumu (prema kojem će Hrvatski sabor o prijedlogu za promjenu Ustava, o prijedlogu zakona ili drugom pitanju iz svojeg djelokruga raspisati referendum ako to zatraži deset posto od ukupnog broja birača u RH), a na osnovi navedenih akata Hrvatskog sabora i Vlade Republike Hrvatske donesenih temeljem članka 127. stavka 2. Poslovnika Hrvatskog Sabora, odnosno temeljem članka 31. stavka 3. Zakona o Vladi Republike Hrvatske, zatražena je kontrola, odnosno provjera broja i vjerodostojnosti potpisa birača te zakonitosti postupka prikupljanja potpisa birača i to od strane Ministarstva uprave kao koordinacijskog tijela, u čiju nadležnost spada provedba Zakona o referendumu, kao i Zakona o registru birača („Narodne novine“ broj 144/12, 105/15).

Takva obrada osobnih podataka u svrhu provjere broja i vjerodostojnosti potpisa birača, predstavlja ne samo provedbu načela točnosti (članak 5.1.d) Opće uredbe o zaštiti podataka), odnosno poštovanje pravnih obveza voditelja obrade (članak 6.1.c) Opće uredbe o zaštiti podataka) već i izvršavanje zadaće od javnog interesa i izvršavanje službenih ovlasti (članak 6.1.e) Opće uredbe o zaštiti podataka) svih nadležnih državnih tijela koji su uključeni u predmetni postupak, tj. provedbu Zakona o referendumu, kao posebnog zakona, odnosno utvrđivanje ukupnog broja potpisa koji su potrebni za raspisivanje referenduma u smislu članka 3. Zakona o referendumu.

Što se tiče povjeravanja poslova obrade osobnih podataka društvu APIS IT d.o.o., kao izvršitelju obrade, navodimo kako se isti poslovi povjeravaju izvršitelju obrade temeljem ugovora ili drugog pravnog akta (odredbe članka 28. Opće uredbe o zaštiti podataka). Napominjemo kako su u ovom slučaju Ministarstvo uprave (naručitelj) i APIS IT d.o.o. (izvršitelj) sklopili Ugovor za uslugu provjere broja i vjerodostojnosti svih potpisa birača iz zahtjeva za raspisivanje državnog referenduma Građanske inicijative: „Narod odlučuje“ o dopuni Ustava Republike Hrvatske člankom 72.a, i „Narod odlučuje“ o izmjeni članka 72. Ustava Republike Hrvatske te Građanske inicijative „Istina o Istanbulskoj“. Također, napominjemo kako izvršitelj obrade (u ovom slučaju društvo APIS IT d.o.o.) obrađuje osobne podatke u ime voditelja obrade, te se u tom slučaju ne smatra da je izvršitelj obrade treća osoba kojoj su dostavljeni osobni podaci, a isto tako dostavljanje osobnih podataka izvršitelju obrade nije potrebno propisati odredbama posebnog zakona. Iz svega navedenoga, proizlazi da se u konkretnom slučaju ne radi o obradi (dostavi) osobnih podataka građana neovlaštenim trećim osobama, već ovlaštenim tijelima (koja su sukladno posebnim zakonima voditelji obrade osobnih podataka), odnosno ovlaštenom društvu (kao izvršitelju obrade sukladno članku 28. Opće uredbe o zaštiti podataka).

Za svaku obradu osobnih podataka mora postojati zakonita svrha te najmanje jedna od relevantnih pravnih osnova u smislu članka 6. Opće uredbe o zaštiti podataka, pri tome je potrebno naglasiti da u slučaju postojanje pravne osnove iz navedenog članka (u konkretnom slučaju postoji pravna osnova nadležnih tijela radi poštivanja pravne obveze i izvršavanje zadaće od javnog interesa i službenih ovlasti) za takvu daljnju obradu osobnih podataka nije potrebna privola osobe čiji se osobni podaci u konkretnom slučaju obrađuju.

Mišljenje 2 – iskazivanje dijagnoze na liječničkom nalazu

U predmetu iskazivanje osobnih podataka (dijagnoze) na liječničkom nalazu, odnosno sumnje u točnost navedene dijagnoze, Agencija je dala mišljenje kako je u konkretnom slučaju u primjeni je Zakon o liječništvu (NN, br. 121/03, 117/08), kao poseban zakon, koji u odredbama članka 4. propisuje kako je u procesu donošenja odluka i izbora dijagnostike i odgovarajućeg liječenja liječnik samostalan u postupanju sukladno znanstvenim saznanjima i stručno dokazanim metodama koje odgovaraju suvremenom standardu struke.

Zakonom o liječništvu propisano je kako se svi postupci medicinske prevencije, dijagnostike i liječenja moraju planirati i provoditi tako da se očuva ljudsko dostojanstvo, integritet osobe i prava pacijenata, a posebno pravo na informiranost i samostalno odlučivanje. Liječnik je dužan u odnosu prema pacijentima postupati primjenjujući i poštujući odredbe posebnih zakona koji reguliraju prava pacijenata te odredbe Kodeksa Hrvatske liječničke komore.

Što se tiče posebnih zakona koji reguliraju prava pacijenata, u primjeni je Zakon o zaštiti prava pacijenata (NN, br. 169/04., 37/08.), koji, uz ostala prava pacijenata, u svojim odredbama propisuje kako pacijent ima uvijek pravo tražiti drugo stručno mišljenje o svome zdravstvenom stanju.

Stoga u konkretnom slučaju ova Agencija nije nadležna preispitivati dijagnoze navedene na nalazu koji je izdao ovlašteni liječnik temeljem obavljenog medicinskog (stručnog) pregleda. Naime, liječnik je ovlašten i dužan postupati sukladno pravilima struke poštujući odredbe gore navedenih posebnih zakona, te odredbe Kodeksa Hrvatske liječničke komore, kao i Kodeksa medicinske etike i deontologije. Zbog postupanja liječnika protivno pravilima struke predviđena je disciplinska odgovornost liječnika (Glava IX Zakona o liječništvu), te je takvo postupanje liječnika moguće prijaviti nadležnim tijelima (Hrvatska liječnička komora).

U tom smislu stranka je upućena kako u svojstvu pacijenta sukladno članku 10. Zakona o zaštiti prava pacijenata ima pravo o svome zdravstvenom stanju zatražiti drugo stručno mišljenje, tj. budući da ova Agencija nije nadležna postupati u odnosu na konkretan slučaj, stranka je upućena da svoja prava (u ovom slučaju prava koja ima u svojstvu pacijenta) može ostvariti na način propisan odredbama gore navedenih posebnih zakona.

Mišljenje 3 – objava osobnih podataka djece na web stranici trgovačkog centra

Agenciji se obratila Pravobraniteljica za djecu, navodeći kako je obaviještena o natječaju za izbor dječjeg modela jednog trgovačkog centra, a koji je proveden putem Facebook stranice organizatora/trgovačkog centra i na kojoj su roditelji objavljivali fotografije svoje djece od 4 do 14

godina, uz navođenje imena i prezimena djeteta, prebivališta te konfekcijskog broja odjeće i veličine obuće djeteta radi natječaja za sudjelovanje u modnoj reviji.

U konkretnom slučaju Agencija je dala mišljenje kako se radi o objavi osobnih podataka djece od strane roditelja, kao njihovih zakonskih zastupnika koji su sukladno odredbama Obiteljskog zakona (NN, br. 103/15.), kao posebnog zakona, dužni skrbiti o djetetovim osobnim i imovinskim pravima te voditi računa o njegovoj dobrobiti u skladu s razvojnim potrebama i mogućnostima djeteta (članak 91. Obiteljskog zakona).

Isto razumijeva da o najboljem interesu djeteta prvenstveno brinu njegovi roditelji/skrbnici, a tek potom institucije i ostali subjekti, kao i društvo u cjelini.

Što se tiče subjekata koji obrađuju osobne podatke djece (voditelji obrade) s aspekta pravnog okvira zaštite osobnih podataka, navodimo kako voditelj obrade (u ovom slučaju Trgovački centar Zagreb d.o.o.) mora poštivati standarde i načela iz Opće uredbe o zaštiti podataka, vodeći računa da svrha u koju se osobni podaci obrađuju bude zakonita i opravdana (članak 5.1.b) Opće uredbe o zaštiti podataka) te da za obradu osobnih podataka postoji pravni temelj (u ovom slučaju pravni temelj za obradu/objavu navedenih osobnih podataka je privola roditelja/skrbnika djeteta u smislu članka 6.1.a) Opće uredbe o zaštiti podataka).

Također, razumijeva se da voditelj obrade koji obrađuje osobne podatke djece (u ovom slučaju Trgovački centar Zagreb d.o.o.) mora voditi računa o tome da djeca zaslužuju posebnu zaštitu u pogledu svojih osobnih podataka, međutim u uvjetima u kojima su roditelji dali privolu za obradu (objavu) osobnih podataka djeteta u navedenu svrhu, razumijeva se da upravo roditelji, koji sukladno posebnom zakonu imaju obvezu štiti prava i interese djeteta, preuzimaju punu odgovornost i u odnosu na zaštitu privatnosti i obradu osobnih podataka djeteta, odnosno njihovu objavu na društvenim mrežama. Dodatno navodimo kako su u ovom slučaju roditelji informirani o uvjetima predmetnog natječaja (koji su objavljeni na navedenoj Facebook stranici), odnosno dostavi i daljnjoj obradi osobnih podataka djece, što razumijeva da su u potpunosti svjesni mogućih rizika vezano uz obradu osobnih podataka u konkretnom slučaju.

Stoga, uvažavajući kako se u konkretnom slučaju radi o dobrovoljnoj objavi osobnih podataka djece od strane njihovih roditelja u određenu (navedenu) svrhu, ne nalazimo da bi se u konkretnom slučaju radilo o nezakonitoj obradi (objavi) osobnih podataka, koja bi bila protivna Općoj uredbi o zaštiti podataka.

Mišljenje 4 – obrada osobnih podataka koju provode agencije za naplatu potraživanja

Agencija za zaštitu osobnih podataka zaprimila je upit vezan za obradu osobnih podataka u svrhu naplate dospjelih, a nenaplaćenih tražbina od strane društava/agencija za naplatu potraživanja sukladno odredbama Opće uredbe o zaštiti podataka, iznosimo sljedeći načelan odgovor: Ističemo kako se od 25. svibnja 2018., u svim državama članicama Europske unije, pa tako i u Republici Hrvatskoj, izravno primjenjuje Uredba (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) SL EU L119.

Navedena Opća uredba o zaštiti podataka u članku 4. stavak 1. točka 1. propisuje da su osobni podaci svi podaci koji se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi, a

pojedinač čiji se identitet može utvrditi jest osoba koja se može identificirati izravno ili neizravno, osobito uz pomoć identifikatora kao što su ime, identifikacijski broj, podaci o lokaciji, mrežni identifikator ili uz pomoć jednog ili više čimbenika svojstvenih za fizički, fiziološki, genetski, mentalni, ekonomski, kulturni ili socijalni identitet tog pojedinca.

Sukladno članku 5. Opće uredbe, osobni podaci moraju biti zakonito, pošteno i transparentno obrađivani s obzirom na ispitanika, prikupljeni u posebne, izričite i zakonite svrhe, primjereni, relevantni i ograničeni na ono što je nužno u odnosu na svrhe u koju se obrađuju, točni i prema potrebi ažurni.

Sukladno članku 6. Opće uredbe o zaštiti podataka obrada je zakonita samo ako i u onoj mjeri u kojoj je ispunjeno najmanje jedno od sljedećega: ispitanik je dao privolu za obradu svojih osobnih podataka u jednu ili više posebnih svrha; obrada je nužna za izvršavanje ugovora u kojem je ispitanik stranka ili kako bi se poduzele radnje na zahtjev ispitanika prije sklapanja ugovora; obrada je nužna radi poštovanja pravnih obveza voditelja obrade; obrada je nužna kako bi se zaštitili ključni interesi ispitanika ili druge fizičke osobe; obrada je nužna za izvršavanje zadaće od javnog interesa ili pri izvršavanju službene ovlasti voditelja obrade; obrada je nužna za potrebe legitimnih interesa voditelja obrade ili treće strane, osim kada su od tih interesa jači interesi ili temeljna prava i slobode ispitanika koji zahtijevaju zaštitu osobnih podataka, osobito ako je ispitanik dijete.

Sukladno načelima poštene i transparentne obrade Opća uredba o zaštiti podataka zahtijeva da je ispitanik informiran o postupku obrade i njegovim svrhama, stoga Vas upućujemo na odredbe članka 13. Opće uredbe o zaštiti podataka kojim je propisano koje je sve informacije voditelj obrade dužan pružiti svojim ispitanicima ako se osobni podaci prikupljaju od ispitanika odnosno na odredbe članka 14. ukoliko osobni podaci nisu dobiveni od ispitanika.

Navodimo kako se određena društva/agencije za naplatu potraživanja, između ostalog, bave poslovima naplate potraživanja odnosno poslovima otkupa potraživanja te se u Vašem slučaju može raditi o povjeravanju određenih poslova izvršitelju obrade putem ugovora/drugog pravnog akta ili o prijenosu tražbina s jednog vjerovnika na drugog vjerovnika (primjerice s banke/teleoperatera na društvo/agenciju za naplatu potraživanja) putem ugovora o cesiji. U nastavku odgovora objašnjavamo oba slučaja.

- a) Povjeravanje određenih poslova izvršitelju obrade putem ugovora/drugog pravnog akta. Člankom 4. točkom 8. Opće uredbe o zaštiti podataka definiran je izvršitelj obrade kao fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo koje obrađuje osobne podatke u ime voditelja obrade.

U konkretnom slučaju, upućujemo Vas na odredbe članka 28. Opće uredbe o zaštiti podataka koji propisuje da se obrada koju provodi izvršitelj obrade uređuje ugovorom ili drugim pravnim aktom u skladu s pravom Unije ili pravom države članice, koji izvršitelja obrade obvezuje prema voditelju obrade, a koji navodi predmet i trajanje obrade, prirodu i svrhu obrade, vrstu osobnih podataka i kategoriju ispitanika te obveze i prava voditelja obrade.

Uzimajući u obzir najnovija dostignuća, troškove provedbe te prirodu, opseg, kontekst i svrhe obrade, kao i rizik različitih razina vjerojatnosti i ozbiljnosti za prava i slobode pojedinaca, voditelj obrade i izvršitelj obrade provode odgovarajuće tehničke i organizacijske mjere kako bi osigurali odgovarajuću razinu sigurnosti s obzirom na rizik (članak 32. Opće uredbe o zaštiti podataka). Slijedom navedenog, ukoliko je voditelj obrade (primjerice: banka/teleoperater) sukladno članku 28. Opće uredbe o zaštiti podataka temeljem ugovora ili drugog pravnog akta povjerio obavljanje točno određenih poslova obrade osobnih podataka izvršitelju obrade (primjerice: društvu/agenciji

za naplatu potraživanja) koji tu obradu provodi u ime voditelja obrade, takva obrada je zakonita odnosno sukladna članku 6. Opće uredbe o zaštiti podataka.

- b) Prijenos tražbina s jednog vjerovnika na drugog vjerovnika putem ugovora o cesiji. Osim navedenog, zakonita osnova za obradu Vaših osobnih podataka od strane društva/agencije za naplatu potraživanja, sukladno članku 6. Opće uredbe o zaštiti podataka mogao bi predstavljati poseban zakon, Zakon o obveznim odnosima („Narodne novine“, broj: 35/05, 41/08, 125/11, 78/15 i 29/18).

Naime, člankom 80. Zakona o obveznim odnosima reguliran je ustup tražbine (cesija) kao ugovor u kojem se tražbina s jednog vjerovnika može prenijeti na drugog vjerovnika, dok je člankom 82. istog zakona propisano da za ustup tražbine nije potreban pristanak dužnika, već je ustupitelj tražbine dužan obavijestiti dužnika o ustupanju.

S tim u vezi navodimo da sam ustup tražbine pretpostavlja i dostavljanje (obradu) osobnih podataka, odnosno ustupanje nije provedivo u praksi ako novi vjerovnik ne zna prema kome ima svoje novostečeno pravo potraživanja. Dakle, provedba instituta cesije nije moguća bez prosljeđivanja osobnih podataka.

Slijedom navedenog, a pod pretpostavkom da se radi o valjanom pravnom poslu sukladno odredbama Zakona o obveznim odnosima (cesiji, otkupu potraživanja i sl.) između voditelja obrade (primjerice: banke/teleoperatera) i nekog društva/agencije za naplatu potraživanja u svrhu naplate dospjelih, a nenaplaćenih tražbina, obrada osobnih podataka od strane društva/agencije za naplatu potraživanja odnosno novog vjerovnika je zakonita.

Nadalje, ističemo kako se informacije o prethodno navedenom odnosno o povjeravanju određenih poslova izvršitelju obrade ili prijenosu tražbina na drugog vjerovnika često nalaze u samom ugovoru, Općim uvjetima poslovanja ili nekom drugom aktu koji Vas kao klijenta/korisnika u potpunosti obvezuje, a što sukladno člancima 13. i 14. Opće uredbe o zaštiti podataka predstavlja informiranje Vas kao klijenta/korisnika.

Također, moramo naglasiti kako je sukladno svojim zakonskim ovlastima ova Agencija nadležna za praćenje i provođenje primjene Opće uredbe o zaštiti podataka u vezi sa obradom osobnih podataka te sukladno svojim ovlastima nije nadležna za tumačenje posebnih postupaka pred za to nadležnim tijelima koji se vode sukladno posebnim propisima (primjerice: utvrđivanje visine konkretnog duga odnosno tražbine).

Zaključno, za svaku obradu osobnih podataka mora postojati relevantna zakonita osnova iz članka 6. Opće uredbe o zaštiti osobnih podataka te izričita, zakonita svrha u koju se osobni podaci obrađuju, a voditelj i izvršitelj obrade su dužni, sukladno članku 32. Opće uredbe o zaštiti podataka provoditi odgovarajuće tehničke i organizacijske mjere kako bi se osigurala odgovarajuća razina sigurnosti osobnih podataka. Vezano uz navedeno, voditelj ili izvršitelj obrade su prilikom komunikacije s klijentom/korisnikom u obvezi nedvojbeno utvrditi njegov identitet kako ne bi došlo do zlouporabe osobnih podataka, a što nužno podrazumijeva davanje/obradu osobnih podatka. Pri tome bi voditelj i izvršitelj obrade trebali poštivati pravo na privatnost u širem smislu te savjesno, pouzdano i odgovorno obrađivati samo osobne podatke stvarnog dužnika, a ne trećih osoba.

Naposljetku, svatko tko smatra da mu je povrijeđeno neko pravo zajamčeno Zakonom o provedbi Opće uredbe o zaštiti podataka („Narodne novine“, broj 42/18) i Općom uredbom o zaštiti podataka, može se sukladno članku 34. obratiti ovoj Agenciji sa zahtjevom za utvrđivanje povrede prava.

Mišljenje 5 – prijenos osobnih podataka zaposlenika tijela javne vlasti u drugu državu članicu Europske unije

Agenciji se obratilo tijelo javne vlasti Republike Hrvatske sa upitom o pravnom temelju za prijenos osobnih podataka svojih zaposlenika u drugu državu članicu Europske unije. Agencija se očitovala kako slijedi:

Načela obrade osobnih podataka, sukladno članku 5. Opće uredbe, traže da osobni podaci moraju biti zakonito, pošteno i transparentno obrađivani s obzirom na ispitanika; prikupljeni u posebne, izričite i zakonite svrhe te se dalje ne smiju obrađivati na način koji nije u skladu s tim svrhama; primjereni, relevantni i ograničeni na ono što je nužno u odnosu na svrhe u koje se obrađuju; točni i prema potrebi ažurni; čuvani u obliku koji omogućuje identifikaciju ispitanika samo onoliko dugo koliko je potrebno u svrhe radi kojih se osobni podaci obrađuju; i obrađivani na način kojim se osigurava odgovarajuća sigurnost osobnih podataka, uključujući zaštitu od neovlaštene ili nezakonite obrade te od slučajnog gubitka, uništenja ili oštećenja primjenom odgovarajućih tehničkih ili organizacijskih mjera. Voditelj obrade odgovara za usklađenost sa ovdje navedenim načelima Opće uredbe te je mora biti u mogućnosti dokazati.

Člankom 6., stavkom 1. Opće Uredbe je propisano da je obrada zakonita samo ako i u onoj mjeri u kojoj je ispunjeno najmanje jedno od sljedećega: (a) ispitanik je dao privolu za obradu svojih osobnih podataka u jednu ili više posebnih svrha; (b) obrada je nužna za izvršavanje ugovora u kojem je ispitanik stranka ili kako bi se poduzele radnje na zahtjev ispitanika prije sklapanja ugovora; (c) obrada je nužna radi poštovanja pravnih obveza voditelja obrade; (d) obrada je nužna kako bi se zaštitili ključni interesi ispitanika ili druge fizičke osobe; (e) obrada je nužna za izvršavanje zadaće od javnog interesa ili pri izvršavanju službene ovlasti voditelja obrade; (f) obrada je nužna za potrebe legitimnih interesa voditelja obrade ili treće strane, osim kada su od tih interesa jači interesi ili temeljna prava i slobode ispitanika koji zahtijevaju zaštitu osobnih podataka, osobito ako je ispitanik dijete.

Ako je pravni temelj za obradu osobnih podataka pravna obveza voditelja obrade, ili ako je obrada nužna za izvršavanje zadaće od javnog interesa ili pri izvršavanju službene ovlasti voditelja obrade, tada ta pravna osnova mora biti utvrđena u pravu Unije ili pravu države članice kojem voditelj obrade podliježe, a tom pravnom osnovom mora biti određena i svrha obrade.

Ta pravna osnova može sadržavati posebne odredbe kako bi se prilagodila primjena pravila ove Uredbe, među ostalim opće uvjete kojima se uređuje zakonitost obrade od strane voditelja obrade, vrste podataka koji su predmet obrade, dotične ispitanike, subjekte kojima se osobni podaci mogu otkriti i svrhe u koje se podaci mogu otkriti, ograničavanje svrhe, razdoblje pohrane te aktivnosti obrade i postupke obrade, uključujući mjere za osiguravanje zakonite i poštene obrade.

Za svaku obradu osobnih podataka voditelj obrade, između ostalog, mora utvrditi pravni temelj za istu. To znači da upravo tijelo javne vlasti, kao voditelj obrade, mora utvrditi koje su njene pravne obveze utvrđene u pravu Unije odnosno nacionalnom zakonodavstvu.

Ako je nekim pravnim propisom propisana Vaša obveza, kao voditelja obrade, da obrađujete osobne podatke zaposlenika u točno utvrđenu svrhu, kao i sve ostale okolnosti obrade navedene *supra*, tada Vam za navedenu obradu nije potreban i drugi pravni temelj iz članka 6., stavka 1. Opće uredbe jer Vam je upravo taj pravni propis temelj za zakonitu obradu.

Ukoliko nemate pravni temelj – poštivanje pravnih obveza voditelja obrade, tada morate pronaći drugi pravni temelj iz članka 6. kako bi ista bila zakonita.

U mišljenju br. 249 o obradi podataka na radnome mjestu, Radna skupina za zaštitu podataka iz članka 29. Direktive 95/46/EZ iznosi mišljenje da se vrlo vjerojatno privola ne može smatrati zakonitim pravnim temeljem za obradu osobnih podataka zaposlenika ili potencijalnih zaposlenika, osim ako isti mogu obradu odbiti bez štetnih posljedica.

Naime, zaposlenici su rijetko u situaciji da slobodno daju, odbiju ili povuku privolu s obzirom na ovisnost koja proizlazi iz odnosa između poslodavca i zaposlenika. Osim u iznimnim situacijama, poslodavci će se morati oslanjati na neku drugu pravnu osnovu koja nije privola, kao što je potreba za obradom podataka u svrhe njihova legitimnog interesa. Međutim, legitimni interes sam po sebi nije dovoljan da bi imao prednost pred pravima i slobodama zaposlenika. Legitimni interes poslodavca može biti pravna osnova za obradu osobnih podataka zaposlenika samo ako je obrada podataka nužna za zakonitu svrhu i u skladu je s načelima proporcionalnosti i supsidijarnosti.

Neovisno o pravnoj osnovi za obradu podataka, prije početka obrade trebalo bi ispitati proporcionalnost kako bi se razmotrilo je li obrada potrebna radi ostvarenja zakonite svrhe te koje se mjere moraju poduzeti kako bi se osiguralo da su kršenja prava na privatni život i tajnost komunikacija svedena na najmanju moguću mjeru.

Također napominjemo da je člankom 29., stavkom 1. Zakona o radu (NN 93/14 i 127/17) propisano da se osobni podaci radnika smiju prikupljati, obrađivati, koristiti i dostavljati trećim osobama samo ako je to određeno ovim ili drugim zakonom ili ako je to potrebno radi ostvarivanja prava i obveza iz radnog odnosa, odnosno u vezi s radnim odnosom.

Nadalje, člankom 29., stavkom 2. istoga Zakona je određeno da ako je osobne podatke iz stavka 1. ovoga članka potrebno prikupljati, obrađivati, koristiti ili dostavljati trećim osobama radi ostvarivanja prava i obveza iz radnoga odnosa, odnosno u vezi s radnim odnosom, poslodavac mora unaprijed pravilnikom o radu odrediti koje će podatke u tu svrhu prikupljati, obrađivati, koristiti ili dostavljati trećim osobama.

Ujedno Vam želimo napomenuti da se prijenos osobnih podataka u neku drugu zemlju članicu EU, u ovom slučaju u Italiju, ne smatra iznošenjem osobnih podataka u smislu poglavlja V Opće uredbe.

Vezano za Vaše pitanje glede dostavljanja preslike osobne iskaznice Vaših zaposlenika, odnosno kontrolora, drugim tijelima, potrebno je napomenuti da je Zakonom o osobnoj iskaznici (NN 62/15), kao posebnim zakonom, propisano kako je osobna iskaznica elektronička javna isprava kojom hrvatski državljanin dokazuje identitet, hrvatsko državljanstvo, spol, datum rođenja i prebivalište u Republici Hrvatskoj. Dakle, osobna iskaznica javna je isprava koja služi u svrhu nedvojbenog utvrđivanja identiteta ispitanika, te se na taj način sprječava moguća zamjena identiteta i zlouporaba osobnih podataka.

Ovdje Vas također podsjećamo na načelo razmjernosti koje traži da osobni podaci budu primjereni, relevantni i ograničeni na ono što je nužno u odnosu na svrhe u koje se obrađuju. Stoga bi, u konkretnom slučaju, trebalo utvrditi može li se svrha identificiranja odnosno provjere identiteta kontrolora postići na manje invazivan način u smislu da se umjesto dostavljanja preslike njegove osobne iskaznice vrši uvid u istu.

Mišljenje 6 – prijenos osobnih podataka zaposlenika u treće zemlje koje nisu članice EU

Agenciji se obratila pravna osoba sa sjedištem u Republici Hrvatskoj sa pitanjem o pravnom temelju za iznošenje osobnih podataka svojih radnika u treće zemlje (Bosna i Hercegovina, Srbija, Kosovo, Albanija itd.). Agencija se očitovala kako slijedi:

Prvenstveno ističemo da je za svako prikupljanje i obradu osobnih podataka u skladu s Općom uredbom potrebno postojanje pravnog temelja iz članka 6. dok je za prijenos podataka trećim zemljama ili međunarodnim organizacijama potrebno i ispunjenje dodatnih uvjeta iz poglavlja V. Opće uredbe.

U članku 44. Opće uredbe naznačeno je kako se svaki prijenos osobnih podataka u treću zemlju ili međunarodnu organizaciju odvija sukladno odredbama Opće uredbe te samo ukoliko voditelj obrade ili izvršitelj obrade ispunjavaju uvjete utvrđene u odredbama Uredbe vezanim za prijenos osobnih podataka trećim zemljama i međunarodnim organizacijama (poglavlje V).

Naime, prijenos osobnih podataka ne bi smio dovesti do narušavanja razine zaštite pojedinaca osigurane Uredbom.

U tom smislu prijenos osobnih podataka trećim zemljama bit će u skladu s odredbama Opće Uredbe samo ukoliko postoji odluka o primjerenosti (članak 45.) odnosno ukoliko prijenosi podliježu odgovarajućim zaštitnim mjerama (članak 46, 47.).

Tek u slučajevima u kojima nije moguće primijeniti jednu od gore navedenih osnova, rješenje treba potražiti u članku 49. Opće uredbe u kojem su naznačeni slučajevi odstupanja za posebne situacije.

Budući da je razvidno kako za predmetne zemlje koje navodite u svom upitu nije donesena odluka o primjerenosti, ukazujemo Vam da je Europska komisija sukladno članku 26. stavku 4. Direktive 95/46/EZ izdala tri seta standardnih ugovornih klauzula koje su sukladno članku 46. stavku 5. i nadalje u primjeni te su iste dostupne na sljedećem linku https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en.

Imajući u vidu stavak 2. točku (c) članka 46. razvidno je kako navedene klauzule predstavljaju odgovarajuću zaštitnu mjeru te kao takve predstavljaju temelj za siguran prijenos osobnih podataka trećim zemljama. Međutim, ističemo kako je prilikom odabira odgovarajućeg seta standardnih ugovornih klauzula potrebno pravilno definirati ugovorne strane kao voditelje odnosno izvršitelje obrade.

Nadalje, uvodnom odredbom 111 u skladu s člankom 49. propisana je mogućnost prijenosa osobnih podataka u treće zemlje unatoč činjenici da za prijenos nije osigurana adekvatna razina zaštite. Naime, stavkom 1. navedenog članka propisano je da ako ne postoji odluka o primjerenosti u skladu s člankom 45. stavkom 3., ili odgovarajuće zaštitne mjere u skladu s člankom 46., što uključuje obvezujuća korporativna pravila, prijenos ili skup prijenosa osobnih podataka u treću zemlju ili međunarodnu organizaciju ostvaruje se samo pod jednim od taksativno navedenih uvjeta:

(a) ispitanik je izričito pristao na predloženi prijenos nakon što je bio obaviješten o mogućim rizicima takvih prijenosa za ispitanika zbog nepostojanja odluke o primjerenosti i odgovarajućih zaštitnih mjera;

- (b) prijenos je nužan za izvršavanje ugovora između ispitanika i voditelja obrade ili provedbu predugovornih mjera na zahtjev ispitanika;
- (c) prijenos je nužan radi sklapanja ili izvršavanja ugovora sklopljenog u interesu ispitanika između voditelja obrade i druge fizičke ili pravne osobe;
- (d) prijenos je nužan iz važnih razloga javnog interesa;
- (e) prijenos je nužan za postavljanje, ostvarivanje ili obranu pravnih zahtjeva;
- (f) prijenos je nužan za zaštitu životno važnih interesa ispitanika ili drugih osoba ako ispitanik fizički ili pravno ne može dati privolu;
- (g) prijenos se obavlja iz registra koji prema pravu Unije ili pravu države članice služi pružanju informacija javnosti i koji je otvoren na uvid javnosti ili bilo kojoj osobi koja može dokazati neki opravdani interes, ali samo u mjeri u kojoj su ispunjeni uvjeti propisani u pravu Unije ili pravu države članice za uvid u tom posebnom slučaju.

Razmatrajući navedeni članak u korelaciji s uvodnom odredbom 32 važno je upozoriti da bi se privola u smislu odredbi Opće uredbe trebala davati jasnom potvrdom radnjom kojom se izražava dobrovoljan, poseban, informiran i nedvosmislen pristanak ispitanika na obradu određenih osobnih podataka koji se odnose na njega.

Imajući u vidu definiciju privole, ističemo kako se pristanak osoba zaposlenih u određenom društvu ne bi mogao smatrati dobrovoljnim pristankom u smislu odredbi Opće uredbe s obzirom na neravnotežu ovlasti koja se javlja u kontekstu zaposlenja. U tom smislu upućujemo na uvodnu odredbu 43 te na Smjernicu o privoli Radne skupine za zaštitu podataka iz članka 29. koju možete otvoriti putem sljedećeg linka <https://azop.hr/images/dokumenti/217/smjernice-o-privoli.pdf>.

Također, u mišljenju br. 249 o obradi podataka na radnome mjestu, Radna skupina za zaštitu podataka iz članka 29. Direktive 95/46/EZ iznosi mišljenje da se vrlo vjerojatno privola ne može smatrati zakonitim pravnim temeljem za obradu osobnih podataka zaposlenika ili potencijalnih zaposlenika, osim ako isti mogu obradu odbiti bez štetnih posljedica.

Naime, zaposlenici su rijetko u situaciji da slobodno daju, odbiju ili povuku privolu s obzirom na ovisnost koja proizlazi iz odnosa između poslodavca i zaposlenika. Osim u iznimnim situacijama, poslodavci će se morati oslanjati na neku drugu pravnu osnovu koja nije privola.

Dakle, u slučajevima u kojima se prijenos podataka odvija prema članku 49. stavku 1. točki (a) potrebno je da voditelj obrade može dokazati da dana privola udovoljava svim uvjetima naznačenim u odredbama Opće uredbe, što u kontekstu zaposlenja, zbog odnosa ovisnosti između radnika i poslodavca, neće biti primjenjivo. Iz tog razloga smatramo kako u takvom odnosu podređenosti privola ne predstavlja adekvatni pravni temelj za prijenos osobnih podataka. Nadalje, primjena članka 49. stavka 1. točke (b) bila bi moguća ukoliko bi navedeni prijenos osobnih podataka u treće zemlje bio povremen. Naime, potrebno je utvrditi učestalost takvog prijenosa s obzirom da članak 49. ne može predstavljati pravni temelj za kontinuirani i ponavljajući prijenos osobnih podataka budući da se primjenom navedenih odredbi smanjuje razina zaštite pojedinca vezano uz obradu njegovih osobnih podataka. S tim u vezi upućujemo Vas na smjernicu koju možete pronaći putem sljedećeg linka:

https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf.

Imajući u vidu kako se iz Vašeg upita može razabrati kako Vaše društvo, u okviru obavljanja svojih djelatnosti, učestalo i ponavljano prenosi osobne podatke zemljama bez odgovarajuće razine zaštite osobnih podataka, Agencija smatra kako članak 49. Opće uredbe ne bi mogao predstavljati pravni temelj za navedene prijenose.

S tim u vezi, Agencija navodi kako je u konkretnom slučaju moguća primjena standardnih ugovornih klauzula odobrenih od strane Europske komisije, a ujedno Vas upućuje na mogućnost sastavljanja kodeksa ponašanja, ugovornih klauzula te obvezujućih korporativnih pravila, sukladno odredbama članka 46. i 47. Opće uredbe.

Agencija također ističe da se u slučaju kad ispitanik sam (u konkretnom slučaju radnik, a primjerice radi potrebe izdavanja dozvola za boravak i rad) dostavlja svoje osobne podatke u inozemstvo, ne radi o prijenosu osobnih podataka u smislu Poglavlja V Opće uredbe.

Mišljenje 7 – prijenos registarskih oznaka u druge države članice EU

Agenciji se obratila pravna osoba sa sjedištem u Republici Hrvatskoj sa upitom o pravnom temelju za prijenos registarskih oznaka u druge države članice Europske unije. Agencija se očitovala kako slijedi:

Uredba (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 - Opća uredba o zaštiti podataka - GDPR je u cijelosti obvezujuća i izravno se primjenjuje u Republici Hrvatskoj od 25. svibnja 2018. godine.

Nastavno na Vaš upit, Agencija najprije ističe da se iznošenje osobnih podataka iz Republike Hrvatske u druge države Europske unije ne smatra iznošenjem u smislu poglavlja V Opće uredbe. Nadalje, člankom 1., stavkom 3. Opće uredbe je propisano da se slobodno kretanje osobnih podataka unutar Unije ne ograničava ni zabranjuje iz razloga povezanih sa zaštitom pojedinaca u pogledu obrade osobnih podataka.

Registarska oznaka je osobni podatak sukladno Općoj uredbi te se njeno iznošenje u treće zemlje odnosno međunarodne organizacije smatra prijenosom osobnih podataka sukladno Općoj uredbi. Nadalje, prijenosi u treće zemlje i međunarodne organizacije mogu se obavljati isključivo uz puno poštovanje ove Uredbe. Prijenos bi se smio obavljati isključivo ako, u skladu s drugim odredbama ove Uredbe, voditelj obrade ili izvršitelj obrade ispunjavaju uvjete utvrđene u odredbama ove Uredbe vezanim za prijenos osobnih podataka trećim zemljama ili međunarodnim organizacijama. Unošenje osobnih podataka u Republiku Hrvatsku nije sporno s aspekta zaštite osobnih podataka. Napominjemo da, sukladno članku 58., stavku 2., točki j) Opće uredbe, Agencija ima korektivnu ovlast narediti suspenziju protoka podataka primatelju u trećoj zemlji. Također, Agencija ima ovlast, sukladno članku 83., stavku 5., točki c), izreći upravnu novčanu kaznu za kršenje odredbi o prijenosu osobnih podataka primatelju u trećoj zemlji.

PREPORUKE, SAVJETI I MIŠLJENJA ZA UNAPRJEĐIVANJE ZAŠTITE OSOBNIH PODATAKA DANI UNUTAR NADZORNIH AKTIVNOSTI AGENCIJE

Unutar nadzornih aktivnosti u širem smislu, pored provedbe nadzora nad obradom osobnih podataka Agencija daje i savjete u svezi s uspostavom novih zbirki osobnih podataka, osobito u slučaju uvođenja nove informacijske tehnologije, prati primjenu organizacijskih i tehničkih mjera za zaštitu podataka te predlaže poboljšanje tih mjera i daje prijedloge i preporuke za unaprjeđivanje zaštite osobnih podataka tj. operativno primjenjuje savjetodavnu komponentu unutar ovlasti koje ima kao nadzorno tijelo.

U nastavku je prikazano nekoliko karakterističnih primjera u kojima su službenici Agencije uputili voditelje/izvršitelje obrade u postupanje za uklanjanje uočenih nedostataka i/ili nepravilnosti ili potencijalnih rizika odnosno dali prijedloge za poboljšanje ili preporuke za unaprjeđenje mjera zaštite osobnih podataka:

U predmetu voditelja obrade - Hrvatski zavod za zdravstveno osiguranje (dalje u tekstu: Zavod) – dani su prijedlozi i preporuke za unaprjeđenje organizacijskih i tehničkih mjera za zaštitu osobnih podataka te poboljšanje istih kao i unaprjeđenje zaštite osobnih podataka: vezano uz pravo i obvezu pregledavati i provjeravati financijske, medicinske i druge podatke u zdravstvenoj ustanovi i kod privatnog zdravstvenog radnika privatne prakse koji imaju sklopljen ugovor sa Zavodom o pružanju usluga zdravstvene zaštite, odnosno ugovornog isporučitelja pomagala, što je izloženo na način da radi učinkovitijeg provođenja zakonom utvrđene kontrole kod ugovornih poslovnih partnera, te posebice zbog izbjegavanja ometanja i usporavanja rada u ugovornim ordinacijama Zavoda, nužno je uspostaviti novi način preuzimanja podataka iz osobnih zdravstvenih kartona osiguranih osoba Zavoda na način da doktor kontrolor Zavoda postavi pisani zahtjev sa svrhom i opsegom potrebnih podataka koje mora kontrolirati, a ugovorni doktor Zavoda prema prijedlogu dostavlja na zaštićeni dio Portala www.cezih.hr dijelove osobnih zdravstvenih kartona određenih osiguranih osoba u pdf formatu (u datoteci). Tražene podatke na siguran način preuzima korisnik doktor kontrolor Zavoda, te ih nakon obavljenog uvida uklanja sa zaštićenog Portala i o tome obavještava ugovornog doktora putem rečenog portala. Zaštićenom dijelu portala www.cezih.hr korisnik doktor kontrolor Zavoda može pristupiti isključivo korištenje iskaznice zdravstveno osigurane osobe -isprava 2- „pametna kartica“ Zavoda koja predstavlja vidljiv dio složene sigurnosne infrastrukture, koja između ostalog osigurava kriptiranje prometa između ugovornih poslovnih partnera – ordinacije i središnjeg dijela informacijskog sustava Zavoda gdje se nalazi portal www.cezih.hr. Zaštićenom dijelu portala koji je konfiguriran na način da svaki korisnik ima svoj pretinac, nemoguće je pristupiti bez spomenute „pametne kartice“ i poznavanja PIN-a kojeg svaki korisnik može promijeniti sam. Efikasnost takvog načina poslovanja Zavoda ima cilj izbjegavanja nepotrebnih odlazaka kontrolora Zavoda u ordinacije ugovornih zdravstvenih radnika i oduzimanju vremena, a koje vrijeme ugovorni doktori koriste za pružanje usluga zdravstvene zaštite osiguranim osobama Zavoda. Slijedom navedenog, kako zdravstveni podaci o pacijentu spadaju u posebnu kategoriju osobnih podataka i kako je tim skupinama podataka potrebno posvetiti veću pažnju prilikom obrade i čuvanja podataka mišljenje Agencije je kako bi navedeni podaci već u digitalnim sustavima evidencija osobnih zdravstvenih kartona pacijenata trebali biti pohranjeni u kriptiranom obliku, a u svrhu dodatnog podizanja razine sigurnosti čuvanja tih podataka. Osim mjera koje se navode u vidu zaštite kriptiranja prometa, preporuča se da podaci zdravstveno osigurane osobe od strane ugovornog doktora Zavoda, koji trebaju biti dostavljeni doktoru kontroloru Zavoda, prilikom dostave u osobni pretinac doktora kontrolora Zavoda budu u kriptiranom obliku kao i da sve vrijeme daljnje obrade dok se ne pobrišu ostanu pohranjena u

pretincu u kriptiranom obliku. Također, preporuča se uvođenje automatiziranog sustava zapisa za evidentiranje radnji (logovi) koje doktor kontrolor Zavoda provodi nad podacima svake osigurane osobe koju je na osnovu svog zahtjeva zaprimio od strane ugovornog doktora Zavoda kao što su npr. pristupanje navedenim podacima, daljnja obrada navedenih podataka, njihovo ispisivanje, umnažanje, daljnje slanje te brisanje. Kako se komunikacija putem elektroničke pošte bez primjene programskog rješenja za enkripciju sadržaja poruke smatra rizičnom i podložnom mogućoj ugrozi i/ili zlouporabi, a kako podaci iz osobnih zdravstvenih kartona osiguranih osoba Zavoda spadaju u posebnu kategoriju osobnih podataka i kako je tim skupinama podataka potrebno posvetiti veću pažnju prilikom obrade i čuvanja podataka preporuča se da se podaci iz osobnih zdravstvenih kartona osiguranih osoba u bilo kakvoj komunikaciji ne dostavljaju putem elektroničke pošte. Osim navedenog USB „stick“ kao medij pohrane podataka, a koji je u pojedinim slučajevima predlagan kao sredstvo pohrane podataka iz osobnih zdravstvenih kartona osiguranih osoba Zavoda prilikom dostavljanja navedenih podataka doktoru kontroloru Zavoda zbog svoje veličine i mogućnosti njegovog gubitka, bez primjene programskog rješenja za enkripciju sadržaja pohranjenog na USB „stick“ i za enkripciju samog USB „sticka“, također se smatra rizičnim medijem za prijenos i dostavu ove posebne skupine osobnih podataka i podložnim mogućoj ugrozi i/ili zlouporabi te se također ne preporuča njegovo korištenje za pohranu i dostavu navedenih podataka.

U predmetu voditelja obrade – Pravobraniteljica za djecu – dani su prijedlozi i preporuke za unaprjeđenje organizacijskih i tehničkih mjera za zaštitu osobnih podataka te poboljšanje istih kao i unaprjeđenje zaštite osobnih podataka: vezano uz zaprimanje i otpremanje neupravnih akata i drugih materijala putem elektroničke pošte a glede obveza utvrđenih i Zakonom o pravobranitelju za djecu (NN 73/17) i Poslovníkom o radu Pravobranitelja za djecu (NN 49/18) da zamjenici Pravobraniteljice za djecu i državni službenici u Uredu pravobraniteljice za djecu dužni su s podacima o djeci postupati u skladu s načelom zaštite najboljeg interesa djeteta te čuvati kao profesionalnu tajnu sve podatke o djeci koje saznaju u obavljanju svojih poslova i ovlasti. Slijedom navedenog, budući da se slanje osobnih podataka bilo koje osobe, a poglavito djece putem elektroničke pošte bez primjene programskog rješenja za enkripciju sadržaja poruke smatra rizičnim i podložnim mogućoj ugrozi i/ili zlouporabi, kako bi se osigurala vrlo visoka razina zaštite osobnih podataka djece prilikom slanja podnesaka iz Ureda pravobraniteljice za djecu putem elektroničke pošte, sa sigurnosnog aspekta tj. glede informacijske sigurnosti za slanje elektroničke pošte čiji je sadržaj po bilo kojem osnovu osjetljive prirode preporučuje se korištenje programskog rješenja za enkripciju podnesaka prije slanja elektroničke drugim tijelima državne uprave i pravnim osobama koje imaju javne ovlasti. Programsko rješenje trebalo bi biti instalirano na svakom računalu u Uredu pravobraniteljice za djecu s kojeg bi se putem elektroničke pošte slao sadržaj koji je po bilo kojem osnovu osjetljive prirode. Treba naglasiti da bi također i primatelji spomenutih poruka/sadržaja trebali imati isto programsko rješenje instalirano na svojim računalima koja zaprimaju elektroničku poštu. Ukoliko druga tijela državne uprave ili pravne osobe koje imaju javne ovlasti imaju potrebu slanja sadržaja, koji je po bilo kojem osnovu osjetljive prirode, prema Uredu pravobraniteljice za djecu, također bi trebali kako bi se osigurala vrlo visoka razina zaštite osobnih podataka djece enkriptirati sadržaj prije slanja elektroničkom poštom. Prije početka slanja prvog enkriptiranog sadržaja, koji je po bilo kojem osnovu osjetljive prirode, sva tijela koja bi sudjelovala u toj komunikaciji, trebala bi Uredu pravobraniteljice za djecu dostaviti svoj tzv. "javni ključ" za enkripciju kog su kreirali pomoću programskog rješenja za enkripciju. Također i Ured pravobraniteljice za djecu trebao bi svim tijelima koja sudjeluju u takvoj komunikaciji dostaviti svoj tzv. „javni ključ“. Nadalje, dodatne tehničko-sigurnosne preporuke za osiguranje visoke razine zaštite komunikacije putem elektroničke pošte između Ureda pravobraniteljice za djecu i drugih tijela državne uprave i pravnih osoba koje imaju javne ovlasti: - Korištenje jakih zaporki za elektroničku poštu, preporučljivo je da zaporka ima minimalno

8 (a preporučljivo je i više) znakova, velika i mala slova, brojeve i barem jedan interpunkcijski znak. Zaporku je preporučljivo mijenjati svakih 3 do 6 mjeseci. Zaporka ne smije sadržavati termine koji mogu biti lako povezivi s korisnikom računa elektroničke pošte (ime, prezime, datum rođenja, adresa, ime članova rodbine, ime kućnih ljubimaca, ...); - Korištenje kriptiranih konekcija na server pošiljatelja elektroničke pošte (za dolazni server SSL/TLS (Secure Sockets Layer/ Transport Layer Security) enkripcija za POP3 (Post Office Protocol) port 995, a za IMAP (Internet Message Access Protocol) port 993, za odlazni server SSL/TLS enkripcija, SMTP (Simple Mail Transfer Protocol) port 465 – oba porta moraju biti otvorena na serveru elektroničke pošte). Za odlazni server (isto kao i za dolazni) mora biti uključena autentifikacija pomoću korisničkog imena i zaporka. Nekriptirane konekcije ne samo da omogućuju eventualnom presretatelju elektroničke pošte uvid u sadržaj elektroničke pošiljke već i mogućnost uvida u korisničko ime i zaporku elektroničke pošte s koje se šalje poruka; - Zaštita iz stavka 2. omogućuje samo zaštitu između računala s kog se šalje elektronička pošta i servera koji se koristi za slanje elektroničke pošte. Stoga se preporuča kriptiranje sadržaja nekim od sustava asimetričnog kriptiranja (sustav javnog i privatnog ključa) Obije strane moraju koristiti isti sustav kriptiranja (i pošiljatelj i primatelj elektroničke pošte); - Program za čitanje i slanje elektroničke pošte mora imati mogućnost prikazivanja poruka upozorenja o promjeni sadržaja dostavljene poruke u odnosu na izvornu poruku; - Ne smiju imati uključenu opciju automatskog dekriptiranja sadržaja poruke i automatskog otvaranja i pokretanja privitaka i/ili Internet poveznica u tekstu elektroničke pošte. Također u programu treba biti isključena opcija prijema (poželjno je i slanja) poruke u HTML (Hypertext Markup Language) obliku već kao čisti (plain) tekst jer u HTML-u može biti sadržan maliciozni dio koji omogućuje eventualnom presretatelju poruke da nakon dekriptiranja elektroničke pošte vidi tekst poruke; - Koristiti pružatelje usluga elektroničke pošte za koje je preporučljivo da: imaju reputaciju sigurnog pružatelja usluga, imaju zaštitu od neželjene pošte (AntiSpam zaštitu), imaju omogućenu autentifikaciju za odlazni server elektroničke pošte, ograničavaju broj (istovremenih) spajanja radi prevencije DoS napada (Denial-of-service attack), imaju zaštitu od DDoS napada (Distributed denial-of-service attack), imaju uključen reverzni DNS (Domain Name System) radi zaštite od lažnih pošiljatelja, koriste DNSBL (Domain Name System-based Blackhole List) servere radi provjere domena i IP adresa pošiljatelja elektroničke pošte kao potencijalnog pošiljatelja neželjene pošte (SPAM), koriste SPF (Sender Policy Framework) metodu (ili neke druge) za otkrivanje nepostojećih adresa pošiljatelja elektroničke pošte, koriste SURBL (Spam URI Real-time Block List) radi otkrivanja elektroničke pošte s nepostojećim ili malicioznim poveznicama (linkovima), kreiraju i koriste takozvane black liste lokalnih korisnika označenih kao distributere neželjene pošte (SPAM), kriptiraju POP3, IMAP i SMTP autentifikaciju korisnika na server (opisane prethodno); također, -Prilikom slanja elektroničke pošte čiji je sadržaj po bilo kojem osnovu osjetljive prirode koristiti žičnu mrežu ureda Pravobraniteljice za djecu i stolna/prijenosna računala na kojim je uspostavljen stupanj zaštite naveden u stavkama 1. do 4.; - Obuka i podizanje svijesti svih dužnosnika i službenika Ureda pravobraniteljice za djecu o važnosti enkripcije podnesaka prije slanja elektronskom poštom i podizanja razine tehničke i informatičke sigurnosti; - Obavezne redovne i pravovremene nadogradnje sustava, programa za slanje i primanje elektroničke pošte i programa za enkripciju. Pri prethodno navedenom preporuke iz stavki 1. i 2. se trebaju implementirati kod svih zaposlenika/korisnika kako bi se eliminirale sigurnosne rupe u komunikacijskom kanalu putem elektroničke pošte. Ukoliko samo jedan zaposlenik/korisnik nema implementirane navedene sigurnosne preporuke predstavlja sigurnosnu prijetnju za neovlašteni ulaz i kompromitiranje sadržaja svih ostalih korisnika u sustavu bez obzira na razinu zaštite implementirane kod njih.

U predmetu voditelja obrade – Ministarstvo uprave – dani su prijedlozi i preporuke za unaprjeđenje organizacijskih i tehničkih mjera za zaštitu osobnih podataka te poboljšanje istih kao i unaprjeđenje zaštite osobnih podataka: vezano uz funkcionalnosti pristupa sustavu e-Građani,

odnosno NIAS, prihvaćanja Općih uvjeta korištenja i nužnosti davanje zasebne privole kod pristupa svakoj usluzi. Slijedom navedenog Agencija je iskazala kako slijedi: prijava na e-usluge obavlja se putem NIAS-a (Nacionalni autentifikacijski i identifikacijski sustav) kroz nekoliko koraka pri čemu NIAS od građana zahtjeva da daju privolu („dozvolu“) za slanje osobnih podataka (ime, prezime i OIB) elektroničkoj usluzi kojoj žele pristupiti. Ukoliko građanin odabere opciju „Ne dozvoli“ proces prijave se obustavlja. Zbog činjenice da postoji mogućnost da je pojedina usluga ili više njih u nadležnosti različitih institucija, i uz pretpostavku da sve osobe ne razumiju u potpunosti kako funkcionira sustav e-Građani, potrebno ih je informirati o funkcioniranju sustava i kojoj instituciji se šalju njezini osobni podaci prilikom odabira određene usluge. Prihvaćanjem Općih uvijete korištenja NIAS-a i davanjem privole osobe potvrđuju informiranost o toj obradi. Također Agencija je stala da je potrebno da funkcionalnost davanja privole osoba bude uključena svaki put kada se pristupa nekoj usluzi e-Građani također i zbog vremenskog odmaka pri čemu se misli na situacije kada osoba nakon što je koristila jednu uslugu, ne pristupi sustavu e-Građani u narednih godinu dana ili više te ju je potrebno ponovo informirati o funkcionalnosti istog. Kako se e-usluzi MojID može pristupiti isključivo sa stranica NIAS-a i poveznica na e-uslugu MojID nije dostupna i lako uočiva u sustavu e-Građani i potrebno je malo više informatičkog znanja i koraka do pristupa navedenoj usluzi, a uz pretpostavku da sve osobe ne razumiju u potpunosti kako funkcionira sustav e-Građani i NIAS, Agencija je mišljenja kako bi u samom sustavu e-Građani bilo potrebno postaviti poveznicu na e-uslugu MojID radi lakšeg podešavanja postavki za skraćeni proces prijave na svaku pojedinu e-uslugu davanjem automatske dozvole za slanje navedenih osobnih podataka.

KARAKTERISTIČNI SLUČAJEVI IZ NADZORNE PRAKSE PROVOĐENJA ZAŠTITE OSOBNIH PODATAKA

Nadzor u sektoru tijela javne vlasti kod voditelja zbirke osobnih podataka: Ministarstvo financija/Porezna uprava, Zagreb, te nadzor u sektoru gospodarstva, kod voditelja zbirke osobnih podataka: FINA – Financijska agencija, Zagreb.

Agencija za zaštitu osobnih podataka (dalje u tekstu: Agencija) zaprimila je pritužbu Udruge BLOKIRANI kojom je „zatraženo“ da Agencija provede istražne, korektivne radnje, da „privremeno zaustavi provedbu i primjenu sljedećih sustava: 1. Sustava javne objave osobnih podataka dužnika Porezne uprave, Ministarstva financija RH; 2. Sustava Jedinog registra računa kojim se kroz FINU obrađuju, objavljuju i trećim licima prenose osobni podaci blokiranih građana; 3. Sustava „agencija za utjerivanje dugova“ (u kontekstu neovlaštene komunikacije do blokiranih građana), jer podnositelj pritužbe smatra da se primjenom gore navedenih sustava „nije vodila posebna briga ni osigurala posebna zaštita osobnih podataka blokiranih građana“. Agencija je, po službenoj dužnosti, tijekom srpnja, kolovoza i rujna 2018. godine, provela izravne i neizravne nadzorne aktivnosti u Ministarstvu financija, Poreznoj upravi, Financijskoj agenciji te analizu prethodnih nadzornih postupanja u odnosu na agencije za naplatu potraživanja.

U provedenom nadzoru u Ministarstvu financija, Poreznoj upravi, nesporno je utvrđeno da je Ministarstvo financija, Porezna uprava, zbog izvršavanja službene ovlasti koja je proizlazila iz tada važeće odredbe članka 8. st. 7. i st. 8. Općeg poreznog zakona („Narodne novine“, 115/2016, dalje u tekstu: OPZ) na Internet stranici Ministarstva financija, objavila Popis dospjelih i neplaćenih dugova, te da je obrada osobnih podataka bila nužna radi izvršavanja službene ovlasti (članak 6. st. 1 e Uredbe (EU) 2016/679 Europskog parlamenta i Vijeća, od 27. travnja 2016. godine 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) SL EU L 119 (dalje u tekstu: Uredba). Slijedom navedenog, takvo postupanje voditelja obrade smatra se zakonitim. Po okončanju nadzora, Agencija, kao savjetodavno tijelo, dostavila je voditelju obrade preporuke vezane za daljnju obradu osobnih podataka vezanim za Popis dospjelih i neplaćenih dugova.

Nadalje, nadzor je obavljen i u Financijskoj agenciji i to posebno na okolnost vođenja Jedinstvenog registra računa koji se vodi u Financijskoj agenciji. Potrebno je napomenuti da je odredbom tada važećeg članka 2. Zakona o provedbi ovrhe na novčanim sredstvima („Narodne novine“ 91/2010 i 112/2012, dalje u tekstu: Zakon) bilo propisano da ovrhu na novčanim sredstvima, na temelju Zakona, provodi Financijska agencija, Hrvatska narodna banka i banke, dok je člankom 4. st. 1. Zakona propisano da se ovrha na novčanim sredstvima ovršenika provodi na novčanim sredstvima u svim bankama, prema osobnom identifikacijskom broju ovršenika, bez njegove suglasnosti i bez obzira ako u osnovi za plaćanje nije određena ovrha na novčanim sredstvima po svim računima i oročenim novčanim sredstvima. Također, u dokaznom postupku je utvrđeno da je vođenje Jedinstvenog registra računa bilo uređeno u skladu s tada važećim odredbama Zakona, tada važećim odredbama Pravilnika o Jedinstvenom registru računa („Narodne novine“, 156/13 i 71/16, dalje u tekstu: Pravilnik), te Uputom o dostavljanju podataka u Jedinstveni registar računa i postupku davanja podataka iz Jedinstvenog registra računa, koju je donijela Uprava Financijske agencije. Slijedom navedenog, razvidno je da je Zakonom propisana obveza vođenja Jedinstvenog registra računa koji vodi Financijska agencija, istim je izričito navedeno da podaci iz Jedinstvenog registra računa koji se odnose na građane nisu javni, a Pravilnikom je, između ostalog, propisan način dostave podataka, uvid u podatke iz Jedinstvenog registra računa te postupanje obveznika dostave podataka u Jedinstveni registar računa. Dakle, prethodno navedena postupanja utemeljena su na Zakonu, te ista nisu bila protivna odredbama Uredbe.

Vodeći računa o navodima iz pritužbe vezanim za „neovlašteno komuniciranje s blokiranim građanima“ provedenom analizom prethodnih nadzornih postupanja u odnosu na agencije za naplatu potraživanja, utvrđeno je da je Zakonom o obveznim odnosima („Narodne novine“, 35/05, 41/08, 125/11, 78/15 i 29/18, dalje u tekstu: ZOO), člancima 80. do 89. ZOO-a, reguliran institut ustupa tražbine. Odredbom članka 80. st. 1. ZOO-a, propisano je, između ostalog, da vjerovnik može ugovorom sklopljenim s trećim prenijeti na ovoga svoju tražbinu, osim one čiji je prijenos zabranjen zakonom ili koja je strogo osobne naravi, ili koja se po svojoj naravi protivi prenošenju na drugoga, dok je odredbom članka 82. st. 1. ZOO-a, propisano da za ustup tražbine nije potreban pristanak dužnika, ali je ustupitelj dužan obavijestiti dužnika o ustupanju. Iz prethodno navedenog proizlazi da je ugovor o cesiji, koji je sklopljen između ustupitelja potraživanja i primatelja potraživanja (agencije za naplatu potraživanja) pravni temelj za obradu osobnih podataka dužnika. Dakle, agencije za naplatu potraživanja, kao voditelji obrade, temelje obradu osobnih podataka dužnika na sklopljenom ugovoru o cesiji, uz napomenu da sam ustup tražbine pretpostavlja i uporabu (obradu) osobnih podataka dužnika. Također, agencije za naplatu potraživanja mogu, na temelju ugovora o nalogu (članak 763. ZOO-a), obavljati poslove naplate potraživanja u ime i za račun nalogodavca. Nastavno na navedeno, pravni temelj za obradu osobnih podataka dužnika može biti i ugovor o nalogu, u kojem slučaju je agencija za naplatu potraživanja izvršitelj obrade, a voditelj obrade je nalogodavac (npr. banka, teleoperator i dr.). Dakle, ako bi se obrada osobnih podataka temeljila na valjano sklopljenim ugovorima o cesiji te

ugovorima o nalogu, obrada osobnih podataka ne bi bila protivna odredbama Uredbe. Međutim, potrebno je napomenuti da bi se u kontekstu neovlaštene komunikacije s blokiranim građanima, u svakom pojedinom slučaju trebao provesti nadzor (na temelju zahtjeva/pritužbe ispitanika, u kojem je potrebno između ostaloga konkretno navesti o kojoj agenciji za naplatu potraživanja je riječ, kao i o kakvoj vrsti neovlaštene komunikacije se točno radi), kako bi se nesporno utvrdilo je li eventualno takvo postupanje, u svakom pojedinom slučaju, poduzimano od strane agencija za naplatu potraživanja, bilo protivno zakonodavnom okviru zaštite osobnih podataka, tj. odredbama Zakona o provedbi opće uredbe o zaštiti podataka (NN, 42/2018) te Uredbe.

Nadzor u sektoru tijela javne vlasti kod voditelja zbirki osobnih podataka: Ministarstvo uprave, Zagreb.

Na temelju Zahtjeva za zaštitu prava ispitanice iz Zagreba vezano uz obradu osobnih podataka u sklopu web aplikacije CIRCA (eng. Communication and Information resource Centre for Administrations) implementirane u sklopu domene e-hrvatska.hr kojoj je cilj poticanje mobilnosti službenika u državnoj upravi (u konkretno slučaju dostupnost osobnih podataka svih službenika zainteresiranih za premještaj te sukladnost pristupa i razmjene osobnih podataka/dokumenata službenika u državnoj službi radi upravljanja premještaja službenika) obavljen je nadzor te je izvršen uvid u funkcionalnost navedene aplikacije i propise vezane uz postupak dodjele ovlaštenja/mogućnosti pristupa predmetnoj aplikaciji (službenika zainteresiranih za premještaj/službenika u jedinici za ljudske potencijale Ministarstva uprave), način identificiranja korisnika aplikacije, sadržaj obrazaca i opseg dostupnih osobnih podataka korisnicima aplikacije, procedure koje se odnose na informacijsku sigurnost, akt o poslovnoj suradnji sa izvršiteljem obrade vezano uz održavanje predmetne aplikacije/pripadajuće baze podataka te da li su korisnici navedene aplikacije informirani o obradi osobnih podataka u skladu sa pravnim okvirom zaštite osobnih podataka.

Provedenim nadzornim aktivnostima utvrđeno je kako svi registrirani korisnici aplikacije mogu vidjeti osobne podatke svih registriranih korisnika odnosno službenika zainteresiranih za premještaj (i njihove priložene obrasce/dokumente) odnosno ne postoji ograničen uvid u osobne podatke prema određenim kriterijima (npr. omogućen uvid samo administratorima aplikacije ili samo djelatnicima zaposlenim u jedinicama za ljudske potencijale).

Slijedom navedenog, voditelju obrade ukazano je na uputnost uvođenja ograničenja uvida u osobne podatke na korisničkoj razini, uputnost dodatnog informiranja korisnika o cjelokupnoj obradi osobnih podataka, educiranja djelatnika u jedinicama za ljudske potencijale vezano uz informacijsku sigurnost te zaštitu osobnih podataka. Također voditelju obrade ukazano je na potrebu donošenja pisane procedure o postupanju pri registraciji korisnika, provjeri točnosti dostavljenih podataka, njihovom korištenju te ažuriranju i/ili brisanju istih te pisane procedure odnosno na dodjelu ovlaštenja pri radu s aplikacijom CIRCA/pripadajućom bazom podataka, kontrola pristupa podacima (tzv. log files), politika lozinki, sigurnosna pohrana (tzv. backup) te također o potrebi dodatnog obvezivanja na povjerljivost svih djelatnika zaposlenih u obradi osobnih podataka.

Nadzor u sektoru tijela javne vlasti kod voditelja zbirki osobnih podataka: Ministarstvo unutarnjih poslova, Zagreb, te nadzor u sektoru tijela javne vlasti, kod voditelja zbirki osobnih podataka: Ministarstvo financija/Porezna uprava, Zagreb.

Agencija za zaštitu osobnih podataka, kao nadzorno tijelo, provela je neizravne nadzore kod voditelja obrade, odnosno u Ministarstvu unutarnjih poslova i Ministarstvu financija, Poreznoj upravi, i to posebno na okolnost određivanja i dodjeljivanja osobnog identifikacijskog broja podnositeljici zahtjeva (ispitanici). Naime, ispitanica se obratila Agenciji navodeći da nikad nije dobila OIB nego da joj je „dodijeljen OIB druge osobe“. Potrebno je istaknuti da rođeno prezime ispitanice sadržava poseban znak ü.

U provedenim nadzornim aktivnostima utvrđeno je da je Ministarstvo financija, Porezna uprava u trenutku masovnog određivanja i dodjeljivanja OIB-a zatečenim hrvatskim državljanima, 1. siječnja 2009., odredilo i dodijelilo OIB-e, i to na temelju podataka upisanih u Evidenciju dodijeljenih matičnih brojeva građana i Evidenciju prebivališta i boravišta u Republici Hrvatskoj, koje vodi Ministarstvo unutarnjih poslova. U dokaznom postupku utvrđeno je da je OIB dodijeljen i ispitanici.

Nadalje, u vrijeme određivanja i dodjeljivanja OIB-a baza podataka na središnjem Informacijskom sustavu Ministarstva unutarnjih poslova nije podržavala znakove koji nisu bili sastavni dio hrvatske abecede, pa tako niti znak ü, a upis posebnih znakova u službenim evidencijama, koje kao voditelj obrade vodi Ministarstvo unutarnjih poslova, omogućen je od lipnja 2010. Nakon što je u Informacijskom sustavu Ministarstva unutarnjih poslova omogućeno upisivanje posebnih znakova (pa tako i posebnog znaka ü), u službenim evidencijama MUP-a, u travnju 2011., izvršen je ispravak podataka u prezimenu ispitanice. Dakle, nakon uvođenja programskog rješenja kojim je bilo omogućeno upisivanje posebnih znakova, obavljeno je usklađivanje podataka u službenim evidencijama MUP-a i Evidenciji o OIB-u. Vezano uz navedeno, Ministarstvo financija, Porezna uprava, osobno je, u studenom 2011., ispitanici uručilo Potvrdu o OIB-u, u kojoj je naveden OIB ispitanice, te ime i prezime koje je sadržavalo i poseban znak ü.

U konkretnom slučaju, iz ukupnosti svih podataka dostavljenih iz Ministarstva unutarnjih poslova prema Ministarstvu financija, Poreznoj upravi, radi određivanja i dodjeljivanja OIB-a, i to: MBG - a ispitanice, imena i prezimena ispitanice (tada bez posebnog znaka ü), rođenog prezimena (tada bez posebnog znaka ü), datuma mjesta i države rođenja, spola, državljanstva, adrese prebivališta, identifikacijskog dokumenta (vrsta, broj, datum važenja, država izdavanja) osobne iskaznice, utvrđeno je da je ispitanici/fizičkoj određen i dodijeljen samo jedan OIB.

Imajući u vidu da se Opća uredba o zaštiti podataka od 25. svibnja 2018., izravno i u cijelosti obvezujuće primjenjuje i u Republici Hrvatskoj, te da Agencija, kao nadzorno tijelo prati i provodi primjenu Uredbe, nadzornim postupanjem nesporno je utvrđeno da su podaci ispitanice o imenu i prezimenu, koji se vode u službenim evidencijama Ministarstva unutarnjih poslova, te u Evidenciji o OIB-u, usklađeni s podacima o osobnom imenu u matici rođenih te knjizi državljana. Dakle, osobni podaci točni su i ažurni, što je u skladu s odredbom članka 5. 1. d) Uredbe, iz koje proizlazi da osobni podaci moraju biti točni i prema potrebi ažurni, da se mora poduzeti svaka razumna mjera radi osiguravanja da se osobni podaci koji nisu točni, uzimajući u obzir svrhe u koje se obrađuju, bez odlaganja izbrišu ili isprave („točnost“).

Agenciji se obratila pravna osoba sa pitanjem smiju li vlasnici trgovačkih društava sa sjedištem u Republici Hrvatskoj iznositi dokumentaciju istih nakon njihove likvidacije izvan Republike Hrvatske ili se ona fizički mora čuvati isključivo u Republici Hrvatskoj. Agencija se očitovala kako slijedi:

Vežano uz pitanje osobnih podataka navodimo kako je člankom 1. točkom 1. Opće uredbe propisano da se Uredbom utvrđuju pravila povezana sa zaštitom pojedinaca u pogledu obrade osobnih podataka i pravila povezana sa slobodnim kretanjem osobnih podataka dok se točkom 2. istog članka propisuje da se istom štite temeljna prava i slobode pojedinaca, a posebno njihovo pravo na zaštitu osobnih podataka.

Nadalje, člankom 4. točkom 1. Opće uredbe osobni podaci definirani su kao „svi podaci koji se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi („ispitanik“); pojedinac čiji se identitet može utvrditi jest osoba koja se može identificirati izravno ili neizravno, osobito uz pomoć identifikatora kao što su ime, identifikacijski broj, podaci o lokaciji, mrežni identifikator ili uz pomoć jednog ili više čimbenika svojstvenih za fizički, fiziološki, genetski, mentalni, ekonomski, kulturni ili socijalni identitet tog pojedinca“.

Opća uredba o zaštiti podataka u svojoj uvodnoj izjavi 14. navodi da bi se zaštita koja se pruža ovom Uredbom u vezi s obradom osobnih podataka trebala odnositi na pojedince bez obzira na njihovu nacionalnost ili boravište. Ovom se Uredbom ne obuhvaća obrada osobnih podataka koji se tiču pravnih osoba, a osobito poduzetnika koji su ustanovljeni kao pravne osobe, uključujući ime i oblik pravne osobe i kontaktne podatke pravne osobe.

Iz druge rečenice navedene odredbe razvidno je da se Opća uredba o zaštiti podataka ne odnosi na podatke pravnih osoba, a osobito poduzetnika koji su ustanovljeni kao pravne osobe (dakle, ovo ne obuhvaća obrtnike, samostalna zanimanja i fizičke osobe koje imaju položaj poduzetnika). Ista odredba pojašnjava da ime (naziv) i oblik pravne osobe te kontakt podaci iste nisu obuhvaćeni Općom uredbom o zaštiti podataka. Uzimajući za primjer trgovačko društvo XY d.o.o., ime (naziv) koji nije zaštićen Uredbom je XY dok je pravni oblik društvo s ograničenom odgovornošću, a kontakt podaci su adresa sjedišta, telefon, generička adresa e-pošte, faks, itd. S druge strane, svaki podatak koji se odnosi na fizičku osobu, bilo da djeluje u okviru svojih poslovnih aktivnosti ili ne, je osobni podatak koji je zaštićen Općom uredbom o zaštiti podataka, pa su u tom smislu podaci direktora, fizičkih osoba koje preuzimaju ili predaju robu, fizičkih osoba koje sastavljaju ili dostavljaju narudžbenice i drugih osoba zaštićeni navedenim propisom.

S tim u vezi također navodimo da prema praksi Suda EU-a (vidjeti predmete C-615/13P i C-398/15), okolnost da se informacija (osobni podaci) nalazi u kontekstu profesionalne aktivnosti nije takve naravi da bi joj oduzela svojstvo skupa osobnih podataka, a iz predmeta C-398/15 (Manni; t. 34. i naredne) je razvidno da to što se određeni osobni podaci obrađuju u okviru aktivnosti trgovačkih društava, ne ograničava opseg primjene propisa o zaštiti osobnih podataka.

Dakle, ukoliko se radi o poslovnoj dokumentaciji koja sadrži određene osobne podatke, tada se na nju odnosno na njih primjenjuje Opća uredba.

S time u vezi važno je istaknuti da je za svako prikupljanje i obradu osobnih podataka u skladu s Općom uredbom potrebno postojanje pravnog temelja iz članka 6. dok je za prijenos podataka trećim zemljama ili međunarodnim organizacijama potrebno i ispunjenje dodatnih uvjeta iz poglavlja V. Opće uredbe.

Nastavno na navedeno pojašnjavamo kako je člankom 1. točkom 3. Opće uredbe propisano kako se Uredbom ne ograničava niti zabranjuje slobodno kretanje osobnih podataka unutar Unije. Dakle, ukoliko se prijenos osobnih podataka odvija između država članica Europske Unije, tada navedeni prijenos ne podliježe dodatnim zahtjevima iz poglavlja V Opće uredbe.

Člankom 6., stavkom 1. Opće Uredbe propisano je da je obrada zakonita samo ako i u onoj mjeri u kojoj je ispunjeno najmanje jedno od sljedećega:

- (a) ispitanik je dao privolu za obradu svojih osobnih podataka u jednu ili više posebnih svrha;
- (b) obrada je nužna za izvršavanje ugovora u kojem je ispitanik stranka ili kako bi se poduzele radnje na zahtjev ispitanika prije sklapanja ugovora;
- (c) obrada je nužna radi poštovanja pravnih obveza voditelja obrade;
- (d) obrada je nužna kako bi se zaštitili životno važni interesi ispitanika ili druge fizičke osobe;
- (e) obrada je nužna za izvršavanje zadaće od javnog interesa ili pri izvršavanju službene ovlasti voditelja obrade;
- (f) obrada je nužna za potrebe legitimnih interesa voditelja obrade ili treće strane, osim kada su od tih interesa jači interesi ili temeljna prava i slobode ispitanika koji zahtijevaju zaštitu osobnih podataka, osobito ako je ispitanik dijete.

Ako je pravni temelj za obradu osobnih podataka pravna obveza voditelja obrade, tada ta pravna osnova mora biti utvrđena u pravu Unije ili pravu države članice kojem voditelj obrade podliježe, a tom pravnom osnovom mora biti određena i svrha obrade.

Tim pravnim temeljem može biti, između ostalog, određeno i razdoblje pohrane. U svakom slučaju, načelo ograničenja pohrane iz članka 5. stavka 1. točke e) Opće uredbe traži da osobni podaci moraju biti čuvani u obliku koji omogućuje identifikaciju ispitanika samo onoliko dugo koliko je potrebno u svrhe radi kojih se osobni podaci obrađuju.

Osobni podaci mogu se pohraniti na dulja razdoblja ako će se osobni podaci obrađivati isključivo u svrhe arhiviranja u javnom interesu, u svrhe znanstvenog ili povijesnog istraživanja ili u statističke svrhe u skladu s člankom 89. stavkom 1., što podliježe provedbi primjerenih tehničkih i organizacijskih mjera propisanih Općom uredbom radi zaštite prava i sloboda ispitanika.

U članku 44. Opće uredbe naznačeno je kako se svaki prijenos osobnih podataka u treću zemlju ili međunarodnu organizaciju odvija sukladno odredbama Opće uredbe te samo ukoliko voditelj obrade ili izvršitelj obrade ispunjavaju uvjete utvrđene u odredbama Uredbe vezanim za prijenos osobnih podataka trećim zemljama i međunarodnim organizacijama (poglavlje V).

Naime, prijenos osobnih podataka ne bi smio dovesti do narušenja razine zaštite pojedinaca osigurane Uredbom.

U tom smislu prijenos osobnih podataka trećim zemljama bit će u skladu s odredbama Opće Uredbe samo ukoliko postoji odluka o primjerenosti (članak 45.) odnosno ukoliko prijenosi podliježu odgovarajućim zaštitnim mjerama (članak 46, 47.).

Tek u slučajevima u kojima nije moguće primijeniti jednu od gore navedenih osnova, rješenje treba potražiti u članku 49. Opće uredbe u kojem su naznačeni slučajevi odstupanja za posebne situacije.

Budući da u svom dopisu niste naveli u koju bi se državu trebali dostavljati osobni podaci, ističemo kako na sljedećem linku možete pronaći popis zemalja za koje je Europska komisija donijela odluku o primjerenosti razine zaštite: https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en.

Nadalje, ukazujemo da je Europska komisija sukladno članku 26. stavku 4. Direktive 95/46/EZ izdala tri seta standardnih ugovornih klauzula koje su sukladno članku 46. stavku 5. i nadalje u primjeni te su iste dostupne na sljedećem linku https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en.

Imajući u vidu stavak 2. točku (c) članka 46. razvidno je kako navedene klauzule predstavljaju odgovarajuću zaštitnu mjeru te kao takve predstavljaju temelj za siguran prijenos osobnih podataka trećim zemljama. Međutim, ističemo kako je prilikom odabira odgovarajućeg seta standardnih ugovornih klauzula potrebno pravilno definirati ugovorne strane kao voditelje odnosno izvršitelje obrade.

Osim toga, napominjemo kako je člankom 46. i 47. Opće uredbe jasno propisano što se smatra odgovarajućim zaštitnim mjerama u smislu Opće uredbe. U tom kontekstu potrebno je razlikovati zaštitne mjere koje podliježu odobrenju nadležnog nadzornog tijela i one mjere koje već prema samim odredbama Opće uredbe predstavljaju odgovarajuću zaštitu za prijenos osobnih podataka te za iste stoga nije potrebno nikakvo dodatno odobrenje.

Zaključno, napominjemo kako je člankom 49. u skladu s uvodnom odredbom 111 propisana mogućnost prijenosa osobnih podataka u treće zemlje unatoč činjenici da za prijenos nije osigurana adekvatna razina zaštite. Naime, stavkom 1. navedenog članka propisano je da ako ne postoji odluka o primjerenosti u skladu s člankom 45. stavkom 3., ili odgovarajuće zaštitne mjere u skladu s člankom 46., što uključuje obvezujuća korporativna pravila, prijenos ili skup prijenosa osobnih podataka u treću zemlju ili međunarodnu organizaciju ostvaruje se samo pod jednim od taksativno navedenih uvjeta:

- (a) ispitanik je izričito pristao na predloženi prijenos nakon što je bio obaviješten o mogućim rizicima takvih prijenosa za ispitanika zbog nepostojanja odluke o primjerenosti i odgovarajućih zaštitnih mjera;
- (b) prijenos je nužan za izvršavanje ugovora između ispitanika i voditelja obrade ili provedbu predugovornih mjera na zahtjev ispitanika;
- (c) prijenos je nužan radi sklapanja ili izvršavanja ugovora sklopljenog u interesu ispitanika između voditelja obrade i druge fizičke ili pravne osobe
- (d) prijenos je nužan iz važnih razloga javnog interesa;
- (e) prijenos je nužan za postavljanje, ostvarivanje ili obranu pravnih zahtjeva;
- (f) prijenos je nužan za zaštitu životno važnih interesa ispitanika ili drugih osoba ako ispitanik fizički ili pravno ne može dati privolju;
- (g) prijenos se obavlja iz registra koji prema pravu Unije ili pravu države članice služi pružanju informacija javnosti i koji je otvoren na uvid javnosti ili bilo kojoj osobi koja može dokazati neki opravdani interes, ali samo u mjeri u kojoj su ispunjeni uvjeti propisani u pravu Unije ili pravu države članice za uvid u tom posebnom slučaju.

Ističemo kako navedena odstupanja iz članka 49. predstavljaju iznimke te se stoga moraju tumačiti restriktivno. Budući da se primjenom navedenih odredbi smanjuje razina zaštite pojedinca vezano uz obradu njegovih osobnih podataka, potrebno je ispitati nužnost takvog prijenosa za ostvarenje određene zakonite svrhe.

U tom smislu upućujemo na Smjernicu Europskog odbora za zaštitu podataka 2/2018 od 25.05.2018. godine u kojoj su detaljno razrađene i analizirane odredbe članka 49. te su pojašnjeni kriteriji za njegovu primjenu (https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf).

Slijedom svega iznesenog, Agencija ističe kako je prije dostave osobnih podataka ispitanika određenoj fizičkoj ili pravnoj osobi u drugoj državi članici Europske Unije potrebno utvrditi postojanje pravnog temelja za zakonitost obrade iz članka 6. dok je za slučaj prijenosa osobnih podataka izvan Europske Unije potrebno utvrditi i postojanje jednog od temelja za prijenos osobnih podataka u treće zemlje u skladu s poglavljem V Opće uredbe.

Agenciji se obratila odvjetnica iz Zagreba sa pitanjem što sve treba dostaviti Agenciji da se dobije suglasnost za iznošenje osobnih podataka u treće zemlje (konkretno Republiku Srbiju), kako izgleda postupak i koliko traje. Agencija se očitovala kako slijedi:

Prvenstveno ističemo da je za svako prikupljanje i obradu osobnih podataka u skladu s Općom uredbom potrebno postojanje pravnog temelja iz članka 6. dok je za prijenos podataka trećim zemljama ili međunarodnim organizacijama potrebno i ispunjenje dodatnih uvjeta iz poglavlja V. Opće uredbe.

Člankom 6. stavkom 1. Opće Uredbe propisano je da je obrada zakonita samo ako i u onoj mjeri u kojoj je ispunjeno najmanje jedno od sljedećega:

- (a) ispitanik je dao privolu za obradu svojih osobnih podataka u jednu ili više posebnih svrha;
- (b) obrada je nužna za izvršavanje ugovora u kojem je ispitanik stranka ili kako bi se poduzele radnje na zahtjev ispitanika prije sklapanja ugovora;
- (c) obrada je nužna radi poštovanja pravnih obveza voditelja obrade;
- (d) obrada je nužna kako bi se zaštitili životno važni interesi ispitanika ili druge fizičke osobe;
- (e) obrada je nužna za izvršavanje zadaće od javnog interesa ili pri izvršavanju službene ovlasti voditelja obrade;
- (f) obrada je nužna za potrebe legitimnih interesa voditelja obrade ili treće strane, osim kada su od tih interesa jači interesi ili temeljna prava i slobode ispitanika koji zahtijevaju zaštitu osobnih podataka, osobito ako je ispitanik dijete.

Ako je pravni temelj za obradu osobnih podataka pravna obveza voditelja obrade, tada ta pravna osnova mora biti utvrđena u pravu Unije ili pravu države članice kojem voditelj obrade podliježe, a tom pravnom osnovom mora biti određena i svrha obrade.

U članku 44. Opće uredbe naznačeno je kako se svaki prijenos osobnih podataka u treću zemlju ili međunarodnu organizaciju odvija sukladno odredbama Opće uredbe te samo ukoliko voditelj obrade ili izvršitelj obrade ispunjavaju uvjete utvrđene u odredbama Uredbe vezanim za prijenos osobnih podataka trećim zemljama i međunarodnim organizacijama (poglavlje V).

Naime, prijenos osobnih podataka ne bi smio dovesti do narušenja razine zaštite pojedinaca osigurane Uredbom.

U tom smislu prijenos osobnih podataka trećim zemljama bit će u skladu s odredbama Opće Uredbe samo ukoliko postoji odluka o primjerenosti (članak 45.) odnosno ukoliko prijenosi podliježu odgovarajućim zaštitnim mjerama (članak 46, 47.).

Tek u slučajevima u kojima nije moguće primijeniti jednu od gore navedenih osnova, rješenje treba potražiti u članku 49. Opće uredbe u kojem su naznačeni slučajevi odstupanja za posebne situacije.

Budući da Europska komisija nije donijela odluku o primjerenosti razine zaštite u Republici Srbiji, u konkretnom slučaju nije moguća primjena članka 45. Opće uredbe. Ujedno napominjemo kako popis zemalja za koje je donesena odluka o primjerenosti zaštite možete pronaći putem sljedećeg linka https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en.

Nadalje, ukazujemo da je Europska komisija sukladno članku 26. stavku 4. Direktive 95/46/EZ izdala tri seta standardnih ugovornih klauzula koje su sukladno članku 46. stavku 5. i nadalje u primjeni te su iste dostupne na sljedećem linku https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en.

Imajući u vidu stavak 2. točku (c) članka 46. razvidno je kako navedene klauzule predstavljaju odgovarajuću zaštitnu mjeru te kao takve predstavljaju temelj za siguran prijenos osobnih podataka trećim zemljama. Međutim, ističemo kako je prilikom odabira odgovarajućeg seta standardnih ugovornih klauzula potrebno pravilno definirati ugovorne strane kao voditelje odnosno izvršitelje obrade.

Osim toga, napominjemo kako je člankom 46. i 47. Opće uredbe jasno propisano što se smatra odgovarajućim zaštitnim mjerama u smislu Opće uredbe. U tom kontekstu potrebno je razlikovati zaštitne mjere koje podliježu odobrenju nadležnog nadzornog tijela i one mjere koje već prema samim odredbama Opće uredbe predstavljaju odgovarajuću zaštitu za prijenos osobnih podataka te za iste stoga nije potrebno nikakvo dodatno odobrenje.

Stavkom 2. članka 46. Opće uredbe propisano je da odgovarajuće zaštitne mjere bez potrebe za ikakvim posebnim ovlaštenjem nadzornog tijela, mogu pružati: (a) pravno obvezujući i provedivi instrument između tijela javne vlasti ili javnih tijela; (b) obvezujuća korporativna pravila u skladu s člankom 47.; (c) standardne klauzule o zaštiti podataka koje donosi Komisija u skladu s postupkom ispitivanja iz članka 93. stavka 2.; (d) standardne klauzule o zaštiti podataka koje donosi nadzorno tijelo i koje Komisija odobrava u skladu s postupkom ispitivanja iz članka 93. stavka 2.; (e) odobreni kodeks ponašanja u skladu s člankom 40. zajedno s obvezujućim i provedivim obvezama voditelja obrade ili izvršitelja obrade u trećoj zemlji za primjenu odgovarajućih zaštitnih mjera, među ostalim u pogledu prava ispitanika; ili (f) odobreni mehanizam certificiranja u skladu s člankom 42. zajedno s obvezujućim i provedivim obvezama voditelja obrade ili izvršitelja obrade u trećoj zemlji za primjenu odgovarajućih zaštitnih mjera, između ostalog u pogledu prava ispitanika.

Dodatno napominjemo kako je postupak odobravanja kodeksa ponašanja te postupak certificiranja detaljnije reguliran odredbama članaka 40.-42. Opće uredbe dok je ispitivanje i odobravanje obvezujućih korporativnih pravila propisano člankom 47. Opće uredbe. Radi dodatnih informacija vezanih uz podnošenje obvezujućih korporativnih pravila na odobrenje u nastavku Vam donosimo sljedeću poveznicu: https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/binding-corporate-rules_en#approval-of-binding-corporate-rules.

Nadalje, stavkom 3. članka 46. propisano je da ugovorne klauzule između voditelja obrade ili izvršitelja obrade i voditelja obrade, izvršitelja obrade ili primatelja osobnih podataka u trećoj zemlji ili međunarodnoj organizaciji kao i odredbe koje treba unijeti u administrativne dogovore između tijela javne vlasti ili javnih tijela, mogu predstavljati odgovarajuće zaštitne mjere pod uvjetom da to odobri nadležno nadzorno tijelo.

S tim u vezi ističemo kako je prije odobravanja ugovornih klauzula i obvezujućih korporativnih pravila od strane nadležnog nadzornog tijela, potrebno prethodno mišljenje Odbora za zaštitu podataka u smislu članka 64. stavka 1. Opće uredbe. Osim toga, obavještavamo Vas kako su rokovi za usvajanje mišljenja od strane Odbora propisani stavkom 3. spomenutog članka dok je stavkom 7. istog članka propisan rok za daljnje postupanje nadzornog tijela.

Zaključno, napominjemo kako je člankom 49. u skladu s uvodnom odredbom 111 propisana mogućnost prijenosa osobnih podataka u treće zemlje unatoč činjenici da za prijenos nije osigurana adekvatna razina zaštite. Naime, stavkom 1. navedenog članka propisano je da ako ne postoji odluka o primjerenosti u skladu s člankom 45. stavkom 3., ili odgovarajuće zaštitne mjere u skladu s člankom 46., što uključuje obvezujuća korporativna pravila, prijenos ili skup prijenosa osobnih podataka u treću zemlju ili međunarodnu organizaciju ostvaruje se samo pod jednim od taksativno navedenih uvjeta:

- (a) ispitanik je izričito pristao na predloženi prijenos nakon što je bio obaviješten o mogućim rizicima takvih prijenosa za ispitanika zbog nepostojanja odluke o primjerenosti i odgovarajućih zaštitnih mjera;
- (b) prijenos je nužan za izvršavanje ugovora između ispitanika i voditelja obrade ili provedbu predugovornih mjera na zahtjev ispitanika;
- (c) prijenos je nužan radi sklapanja ili izvršavanja ugovora sklopljenog u interesu ispitanika između voditelja obrade i druge fizičke ili pravne osobe
- (d) prijenos je nužan iz važnih razloga javnog interesa;
- (e) prijenos je nužan za postavljanje, ostvarivanje ili obranu pravnih zahtjeva;
- (f) prijenos je nužan za zaštitu životno važnih interesa ispitanika ili drugih osoba ako ispitanik fizički ili pravno ne može dati privolu;
- (g) prijenos se obavlja iz registra koji prema pravu Unije ili pravu države članice služi pružanju informacija javnosti i koji je otvoren na uvid javnosti ili bilo kojoj osobi koja može dokazati neki opravdani interes, ali samo u mjeri u kojoj su ispunjeni uvjeti propisani u pravu Unije ili pravu države članice za uvid u tom posebnom slučaju.

Međutim, ističemo kako navedena odstupanja iz članka 49. predstavljaju iznimke te se stoga moraju tumačiti restriktivno. Budući da se primjenom navedenih odredbi smanjuje razina zaštite pojedinca vezano uz obradu njegovih osobnih podataka, potrebno je ispitati nužnost takvog prijenosa za ostvarenje određene zakonite svrhe. Jednako tako, potrebno je utvrditi učestalost takvog prijenosa s obzirom da članak 49. ne može predstavljati pravni temelj za kontinuirani i ponavljajući prijenos osobnih podataka između dva povezana subjekta. S tim u vezi upućujemo Vas na smjernicu koju možete pronaći putem sljedećeg linka:

https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf.

Slijedom svega iznesenog, Agencija ističe kako je prije dostave osobnih podataka ispitanika određenom poslovnom subjektu u Republici Srbiji potrebno utvrditi postojanje pravnog temelja za zakonitost obrade iz članka 6. te postojanje jednog od temelja za prijenos osobnih podataka u treće zemlje u skladu s poglavljem V Opće uredbe. Dakle, za prijenos osobnih podataka u Republiku Srbiju nije nužno dobivanje suglasnosti Agencije već postojanje adekvatnog pravnog temelja u skladu s odredbama Opće uredbe. S time u vezi napominjemo kako pravni temelj mogu predstavljati postojeće standardne ugovorne klauzule odobrene od strane Europske komisije, dok je za prijenos osobnih podataka putem ugovornih klauzula, kodeksa ponašanja ili obvezujućih korporativnih pravila, potrebna prethodna dostava navedenih isprava na odobrenje Agenciji.

Agenciji se obratilo odvjetničko društvo iz Republike Hrvatske sa upitom može li izvršitelj obrade koji ima poslovni nastan u Republici Hrvatskoj istovremeno biti imenovan predstavnikom voditelja obrade čiji se poslovni nastan nalazi izvan Europske unije. Agencija se očitovala kako slijedi:

Uredba (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 - Opća uredba o zaštiti podataka (dalje u tekstu: Opća uredba) je u cijelosti obvezujuća i izravno se primjenjuje u Republici Hrvatskoj od 25. svibnja 2018. godine te njezine odredbe moraju poštivati svi subjekti koji u sklopu svojih aktivnosti obrađuju osobne podatke fizičkih osoba u Europskoj uniji te u određenim slučajevima i subjekti izvan Europske Unije.

Dakle, sukladno njenom članku 3. stavku 2., Opća uredba se primjenjuje na obradu osobnih podataka ispitanika u Uniji koju obavlja voditelj obrade ili izvršitelj obrade bez poslovnog nastana u Uniji, ako su aktivnosti obrade povezane s nuđenjem robe ili usluga takvim ispitanicima u Uniji, neovisno o tome treba li ispitanik izvršiti plaćanje ili ako su aktivnosti obrade povezane s praćenjem njihova ponašanja dokle god se njihovo ponašanje odvija unutar Unije.

U prethodna dva slučaja, a sukladno članku 27. Opće uredbe, voditelj ili izvršitelj obrade mora pisanim putem imenovati predstavnika u Uniji, osim u slučaju povremene obrade, obrade koja ne uključuje u velikoj mjeri obradu posebnih kategorija podataka iz članka 9. stavka 1. ili obradu osobnih podataka u vezi s kaznenim osudama i kažnjivim djelima iz članka 10. te za koju nije vjerojatno da će prouzročiti rizik za prava i slobode pojedinca ili ako je voditelj obrade tijelo javne vlasti ili javno tijelo.

Nadalje, Opća uredba u uvodnoj odredbi 80 propisuje da bi predstavnik trebao djelovati u ime voditelja obrade ili izvršitelja obrade i da može mu se obratiti svako nadzorno tijelo. Voditelj obrade ili izvršitelj obrade trebao bi izričito, pisanim ovlaštenjem imenovati predstavnika da djeluje u njegovo ime s obzirom na obveze voditelja i izvršitelja obrade na temelju ove Uredbe. Imenovanje takvog predstavnika ne utječe na dužnost i predstavljanje voditelja obrade, odgovornost voditelja obrade ili izvršitelja obrade na temelju ove Uredbe.

Takav bi predstavnik svoje zadaće trebao obavljati u skladu s mandatom dobivenim od voditelja ili izvršitelja obrade, uključujući suradnji s nadležnom tijelom u vezi sa svakom radnjom poduzetom za osiguravanje poštovanja ove Uredbe. U slučaju da voditelj ili izvršitelj obrade krši pravila, imenovani predstavnik bi trebao podlijegati postupku izvršavanja zakonodavstva.

Voditelji obrade koji u EU-u nemaju poslovni nastan moraju poslovati s lokalnim nadzornim tijelima u svakoj državi članici u kojoj djeluju preko svojih lokalnih predstavnika, kako bi se poštovao mehanizam konzistentnosti i suradnje iz Opće uredbe.

Opća uredba u članku 4. stavku 1. točki 7. definira voditelja obrade kao fizičku ili pravnu osobu, tijelo javne vlasti, agencija ili drugo tijelo koje samo ili zajedno s drugima određuje svrhe i sredstva obrade osobnih podataka; kada su svrhe i sredstva takve obrade utvrđeni pravom Unije ili pravom države članice, voditelj obrade ili posebni kriteriji za njegovo imenovanje mogu se predvidjeti pravom Unije ili pravom države članice.

Izvršitelj obrade, prema članku 4. stavku 1. točki 8., jest fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo koje obrađuje podatke u ime voditelja obrade.

Dakle, voditelj određuje svrhu obrade osobnih podataka i provodi odgovarajuće tehničke i organizacijske mjere, kako bi mogao dokazati da se obrada provodi u skladu s Uredbom, dok izvršitelj provodi obradu u ime voditelja. Opća uredba daje mogućnost voditelju obrade da povjeri izvršitelju obrade obavljanje samo nekih točno ugovorenih poslova u ime i za račun voditelja obrade, a ne nameće mu obvezu imenovati izvršitelja obrade.

Međutim, to što izvršitelj na temelju ugovornog odnosa izvršava određenu obradu podataka u ime i za račun voditelja ne znači da izmiče odgovornosti i načelima obrade iz Opće uredbe. Naime, izvršitelj obrade mora jamčiti zaštitu i povjerljivost obrade osobnih podataka te je dužan provoditi odgovarajuće mjere zaštite kako bi osigurao i mogao dokazati da se obrada provodi u skladu s Općom uredbom.

Nadalje, sukladno članku 28. stavku 10. Opće uredbe, ne dovodeći u pitanje članke 82., 83. i 84., ako izvršitelj obrade krši ovu Uredbu utvrđivanjem svrhe i načine obrade podataka, izvršitelj obrade smatra se voditeljem obrade u pogledu te obrade.

Sukladno članku 4. stavku 1. točki 17. predstavnik znači fizička ili pravna osoba s poslovnim nastanom u Uniji koju je voditelj obrade ili izvršitelj obrade imenovao pisanim putem u skladu s člankom 27., a koja predstavlja voditelja obrade ili izvršitelja obrade u pogledu njihovih obveza na temelju ove Uredbe.

Predstavnik voditelja obrade, iz članka 27. Opće uredbe, dužan je obavljati svoje poslove pošteno i savjesno, odgovorno i nepristrano čuvajući vlastitu vjerodostojnost te vjerodostojnost voditelja obrade koga predstavlja, a u odnosu na ispitanike i nadzorno tijelo s kojima mora komunicirati u svim predmetnim stvarima u ime voditelja obrade.

Postoji bojazan da bi izvršitelj obrade stavljao svoje zadaće ispred predstavničkih zadaća nauštrb ispitanika i nadzornog tijela koji bi mu se obraćali sa svojim zahtjevima. Naime, izvršitelj na temelju ugovornog odnosa izvršava određenu obradu podataka u ime i za račun voditelja te predstavlja svojevrsnu produženu ruku voditelja obrade u tehničkom smislu obrade tih podataka. U tom smislu, kada bi izvršitelj obrade predstavljao voditelja obrade, postoji mogućnost nepristranog i nepouzdanog djelovanja u odnosu na ispitanike i nadzorno tijelo.

Slijedom navedenog, kako bi se osiguralo da izvršitelj obrade u ulozi predstavnika voditelja obrade ne bi bio u koliziji u smislu dvije dužnosti, bilo bi uputno uspostaviti procese i praksu u radnom okruženju koji će poticati učinkovitu kontrolu, upravljanje i rješavanje situacija sukoba interesa, stvoriti kulturu otvorene komunikacije i dijaloga koji se odnose na etičnost i trajno ju promicati te omogućiti edukaciju svojih zaposlenika o uspostavljenim standardima.

Međutim, smatramo da bi uspostavljanje navedenih procedura i prevelika kontrola izvršitelja obrade, u smislu predstavničke zadaće, u praksi mogla biti neprovediva i kontraproduktivna što bi rezultiralo nepovjerenjem u voditelja obrade.

Situacije u kojima sukob interesa postoji ili koje mogu dovesti do istog treba izbjegavati u što većoj mjeri. Treba uzeti u obzir činjenicu da kada se govori o sukobu interesa kao problematici, ne smatra se problematičnim samo stvarna zlouporaba u obavljanju poslova, već i sama mogućnost pojave određenog doloznog i nepoželjnog ponašanja. Iz toga razloga Agencija je mišljenja da sukob interesa treba prevenirati prije negoli do istog dođe.

Dakle, izvršitelj obrade koji bi predstavljao voditelja obrade bez poslovnog nastana, u odnosu na ispitanike bio bi interesno nejasan jer bi s jedne strane izvršavao obradu u ime voditelja obrade, a s druge strane predstavljao voditelja za tu istu obradu prema ispitanicima i nadzornom tijelu. U tom smislu do sukoba interesa posebno bi moglo doći kod utvrđivanja odgovornosti izvršitelja - predstavnika s jedne strane te voditelja obrade s druge strane.

Zaključno, predstavnik voditelja obrade služi kao polazišna točka za obradu osobnih podataka voditelja obrade bez poslovnog nastana u Europskoj Uniji. Imajući u obzir navedeno, predstavnik mora biti u stanju učinkovito komunicirati s ispitanicima o obradi osobnih podataka i surađivati s relevantnim nadzornim tijelima za zaštitu osobnih podataka.

Sukladno specifičnim zadaćama, obvezama i interesima predstavnika voditelja obrade i izvršitelja istog voditelja, Agencija smatra kako bi obnašanje dviju funkcija u istoj osobi bilo u koliziji i predstavljalo mogući sukob interesa.

Agenciji se obratila pravna osoba sa sjedištem u Republici Srbiji sa upitom da li se na njih primjenjuje odredba Opće uredbe o imenovanju predstavnika budući da imaju namjeru svoje poslovanje proširiti na Republiku Hrvatsku. Agencija se očitovala kako slijedi:

Uvodna izjava 23 Opće uredbe propisuje sljedeće:

Kako bi se osiguralo da pojedincima nije uskraćena zaštita na koju imaju pravo na temelju ove Uredbe, na obradu osobnih podataka ispitanika koji se nalaze u Uniji, a koju obavlja voditelj obrade ili izvršitelj obrade bez poslovnog nastana u Uniji, trebala bi se primjenjivati ova Uredba ako su aktivnosti obrade povezane s ponudom robe ili usluga takvim ispitanicima, bez obzira na to ima li ta ponuda veze s plaćanjem. Kako bi se utvrdilo nudi li takav voditelj obrade ili izvršitelj obrade robu ili usluge ispitanicima koji se nalaze u Uniji, trebalo bi utvrditi je li očito da voditelj obrade ili izvršitelj obrade namjerava ponuditi usluge ispitanicima koji se nalaze u jednoj ili više država članica Unije. Iako su sama dostupnost internetskih stranica voditelja obrade, izvršitelja obrade ili posrednika u Uniji ili adrese elektroničke pošte i drugih kontaktnih podataka ili korištenje jezikom koji je općenito u uporabi u trećoj zemlji u kojoj voditelj obrade ima poslovni nastan nedovoljni za utvrđivanje takve namjere, čimbenici kao što je korištenje jezikom ili valutom koji su općenito u uporabi u jednoj ili više država članica s mogućnošću naručivanja robe i usluga na tom drugom jeziku, ili spominjanje kupaca ili korisnika koji se nalaze u Uniji, mogu jasno pokazati da voditelj obrade namjerava nuditi robu ili usluge ispitanicima u Uniji.

Nadalje, temeljem uvodne izjave 24, na obradu osobnih podataka ispitanika koji se nalaze u Uniji, a koju obavlja voditelj obrade ili izvršitelj obrade bez poslovnog nastana u Uniji, također bi se trebala primjenjivati ova Uredba kada se odnosi na praćenje ponašanja takvih ispitanika ako se njihovo ponašanje odvija unutar Unije. Kako bi se odredilo može li se aktivnost obrade smatrati praćenjem ponašanja ispitanika, trebalo bi utvrditi prati li se pojedince na internetu među ostalim mogućom naknadnom upotrebom tehnika obrade osobnih podataka koje se sastoje od izrade profila pojedinca, osobito radi donošenja odluka koje se odnose na njega ili radi analize ili predviđanja njegovih osobnih sklonosti, ponašanja i stavova.

Isto je ujedno uređeno i člankom 3. stavkom 2. Opće uredbe (teritorijalno područje primjene):

Ova se Uredba primjenjuje na obradu osobnih podataka ispitanika u Uniji koju obavlja voditelj obrade ili izvršitelj obrade bez poslovnog nastana u Uniji, ako su aktivnosti obrade povezane s:

- a) nuđenjem robe ili usluga takvim ispitanicima u Uniji, neovisno o tome treba li ispitanik izvršiti plaćanje; ili
- b) praćenjem njihova ponašanja dokle god se njihovo ponašanje odvija unutar Unije.

Da bi došlo do eventualne primjene članka 3. stavka 2. Opće uredbe odlučujuće je da se radi o voditelju obrade ili izvršitelju obrade koji nema poslovni nastan u Uniji. Sukladno 22. uvodnoj izjavi Opće uredbe, poslovni nastan podrazumijeva djelotvorno i stvarno obavljanje djelatnosti putem stabilnih aranžmana. Pravni oblik takvih aranžmana, bilo kroz podružnicu ili društvo kćer s pravnom osobnošću, nije odlučujući čimbenik u tom pogledu.

Naime, Opća uredba se, sukladno članku 3. stavku 1., (uvijek) odnosi na obradu osobnih podataka u okviru poslovnog nastana voditelja obrade ili izvršitelja obrade u Uniji, neovisno o tome obavlja li se obrada u Uniji ili ne.

Sukladno članku 4. stavku 1. točki 17), predstavnik znači fizička ili pravna osoba s poslovnim nastanom u Uniji koju je voditelj ili izvršitelj obrade imenovao pisanim putem u skladu s člankom 27., a koja predstavlja voditelja obrade ili izvršitelja obrade u pogledu njihovih obveza na temelju ove Uredbe.

Temeljem članka 27. Opće uredbe, ako se primjenjuje članak 3. stavak 2., voditelj obrade ili izvršitelj obrade pisanim putem imenuju predstavnika u Uniji.

Ova obveza se ne primjenjuje na obradu koja je povremena, ne uključuje u velikoj mjeri obradu posebnih kategorija podataka iz članka 9. stavka 1. ili obradu osobnih podataka u vezi s kaznenim osudama i kažnjivim djelima iz članka 10. te za koju nije vjerojatno da će prouzročiti rizik za prava i slobode pojedinaca uzimajući u obzir prirodu, kontekst, opseg i svrhe obrade.

Također, ova obveza se ne primjenjuje na tijela javne vlasti ili javna tijela.

Predstavnik mora imati poslovni nastan u jednoj od država članica u kojoj se nalaze ispitanici čiji se osobni podaci obrađuju u vezi s robom ili uslugama koje im se nude ili čije se ponašanje prati.

Voditelj obrade ili izvršitelj obrade ovlašćuju predstavnika kako bi se, uz obraćanje voditelju ili izvršitelju obrade ili umjesto obraćanja njima, njemu obraćali osobito nadzorna tijela i ispitanici u pogledu svih pitanja u vezi s obradom za potrebe osiguravanja sukladnosti s Općom uredbom.

Imenovanje predstavnika voditelja obrade ili izvršitelja obrade ne utječe na pravne zahtjeve koji bi mogli biti postavljeni protiv samog voditelja obrade ili izvršitelja obrade.

Navedeno je uređeno i uvodnom izjavom 80 Opće uredbe:

Ako voditelj obrade ili izvršitelj obrade koji nema poslovni nastan u Uniji obrađuje osobne podatke ispitanika u Uniji čije su aktivnosti obrade povezane s ponudom robe ili usluga, bez obzira na to je li potrebno plaćanje ispitanika, za takve bi ispitanike u Uniji, ili za praćenje njihova ponašanja dok se ono odvija unutar Unije, voditelj obrade ili izvršitelj obrade trebali bi imenovati predstavnika, osim ako se obrada obavlja povremeno, ne uključuje opsežnu obradu posebnih kategorija osobnih podataka ili je obrada osobnih podataka povezana s kaznenim presudama i kažnjivim djelima te vjerojatno neće dovesti do rizika za prava i slobode pojedinaca, uzimajući u obzir prirodu, kontekst, opseg i svrhe obrade ili ako je voditelj obrade tijelo javne vlasti ili javno tijelo. Predstavnik bi trebao djelovati u ime voditelja obrade ili izvršitelja obrade i može mu se obratiti svako nadzorno tijelo. Voditelj obrade ili izvršitelj obrade trebao bi izričito, pisanim ovlaštenjem imenovati predstavnika da djeluje u njegovo ime s obzirom na obveze voditelja obrade i izvršitelja obrade na temelju ove Uredbe. Imenovanje takvog predstavnika ne utječe na dužnost ili odgovornost voditelja obrade ili izvršitelja obrade na temelju ove Uredbe. Takav bi predstavnik svoje zadaće trebao obavljati u skladu s mandatom dobivenim od voditelja obrade ili izvršitelja obrade, uključujući suradnju s nadležnim nadzornim tijelima u vezi sa svakom radnjom poduzetom

za osiguravanje poštovanja ove Uredbe. U slučaju da voditelj obrade ili izvršitelj obrade krši pravila, imenovani bi predstavnik trebao podliježati postupku izvršavanja zakonodavstva.

Vežano za Vaše navode iz dopisa da biste osobne podatke izvozili iz Republike Srbije Vašem poslovnom partneru u Republiku Hrvatsku, napominjemo da se na navedeni prijenos osobnih podataka ne primjenjuje poglavlje V Opće uredbe – prijenosi osobnih podataka trećim zemljama ili međunarodnim organizacijama. Poglavlje V Opće uredbe, kako i njegov naziv navodi, primjenjuje se jedino u slučaju prijenaosa osobnih podataka iz EU u neku treću zemlju odnosno međunarodnu organizaciju.

Naime, sukladno 101. uvodnoj izjavi Opće uredbe, kada se osobni podaci prenose iz Unije voditeljima obrade, izvršiteljima obrade ili drugim primateljima u trećim zemljama ili međunarodnim organizacijama, ne bi smjela biti narušena razina zaštite pojedinaca osigurana ovom Uredbom u Uniji, među ostalim u slučajevima daljnjih prijenaosa osobnih podataka iz treće zemlje ili međunarodne organizacije voditeljima obrade, izvršiteljima obrade u istoj ili nekoj drugoj trećoj zemlji ili međunarodnoj organizaciji. U svakom slučaju, prijenosi u treće zemlje i međunarodne organizacije mogu se obavljati isključivo uz puno poštovanje ove Uredbe. Prijenos bi se smio obavljati isključivo ako, u skladu s drugim odredbama ove Uredbe, voditelj obrade ili izvršitelj obrade ispunjavaju uvjete utvrđene u odredbama ove Uredbe vezanim za prijenos osobnih podataka trećim zemljama ili međunarodnim organizacijama.

Dakle, ukoliko bi Vaš poslovni partner iznosio određene osobne podatke iz Republike Hrvatske Vašoj tvrtki u Republiku Srbiju, tada se na navedeni prijenos primjenjuje Opća uredba, odnosno njeno Poglavlje V.

Odvjetnica iz Zagreba se obratila Agenciji u ime svojeg klijenta – pravne osobe sa sjedištem u Republici Hrvatskoj, sa upitom o pravnoj temelju za slanje životopisa svojih zaposlenika potencijalnim klijentima na području Republike Hrvatske, ali i izvan područja Republike Hrvatske. Agencija se očitovala kako slijedi:

Člankom 6., stavkom 1. Opće Uredbe je propisano da je obrada zakonita samo ako i u onoj mjeri u kojoj je ispunjeno najmanje jedno od sljedećega: (a) ispitanik je dao privolu za obradu svojih osobnih podataka u jednu ili više posebnih svrha; (b) obrada je nužna za izvršavanje ugovora u kojem je ispitanik stranka ili kako bi se poduzele radnje na zahtjev ispitanika prije sklapanja ugovora; (c) obrada je nužna radi poštovanja pravnih obveza voditelja obrade; (d) obrada je nužna kako bi se zaštitili ključni interesi ispitanika ili druge fizičke osobe; (e) obrada je nužna za izvršavanje zadaće od javnog interesa ili pri izvršavanju službene ovlasti voditelja obrade; (f) obrada je nužna za potrebe legitimnih interesa voditelja obrade ili treće strane, osim kada su od tih interesa jači interesi ili temeljna prava i slobode ispitanika koji zahtijevaju zaštitu osobnih podataka, osobito ako je ispitanik dijete.

Dalje tumačimo privolu kao mogući pravni temelj za obradu osobnih podataka radnika.

Člankom 4., stavkom 1., točkom 11. definirana je privola kao svako dobrovoljno, posebno, informirano i nedvosmisleno izražavanje želja ispitanika kojim on izjavom ili jasnom potvrdnom radnjom daje pristanak za obradu osobnih podataka koji se na njega odnose.

Uvodna izjava 43 navodi da, kako bi se osiguralo da je privola dana dobrovoljno, ona ne bi smjela predstavljati valjanu pravnu osnovu za obradu osobnih podataka u određenom slučaju kada postoji jasna neravnoteža između ispitanika i voditelja obrade, posebno ako je voditelj obrade tijelo javne vlasti i stoga nije vjerojatno da je s obzirom na sve okolnostima te posebne situacije privola dana dobrovoljno.

Opća Uredba uvjete privole propisuje u članku 7.:

Kada se obrada temelji na privoli, voditelj obrade mora moći dokazati da je ispitanik dao privolu za obradu svojih osobnih podataka. Ako ispitanik da privolu u vidu pisane izjave koja se odnosi i na druga pitanja, zahtjev za privolu mora biti predložen na način da ga se može jasno razlučiti od drugih pitanja, u razumljivom i lako dostupnom obliku uz uporabu jasnog i jednostavnog jezika. Svaki dio takve izjave koji predstavlja kršenje ove Uredbe nije obvezujući. Ispitanik ima pravo u svakom trenutku povući svoju privolu. Povlačenje privole ne utječe na zakonitost obrade na temelju privole prije njezina povlačenja. Prije davanja privole, ispitanika se o tome obavješćuje. Povlačenje privole mora biti jednako jednostavno kao i njezino davanje. Kada se procjenjuje je li privola bila dobrovoljna, u najvećoj mogućoj mjeri uzima se u obzir je li, među ostalim, izvršenje ugovora, uključujući pružanje usluge, uvjetovano privolom za obradu osobnih podataka koja nije nužna za izvršenje tog ugovora.

Nadalje, 32. uvodnom izjavom Preambule Opće Uredbe navedeno je da bi se privola trebala davati jasnom potvrdnom radnjom kojom se izražava dobrovoljan, poseban, informiran i nedvosmislen pristanak ispitanika na obradu osobnih podataka koji se odnose na njega, poput pisane izjave, uključujući elektroničku, ili usmene izjave. To bi moglo obuhvaćati označavanje polja kvačicom pri posjetu internetskim stranicama, biranje tehničkih postavaka usluga informacijskog društva ili drugu izjavu ili ponašanje koje jasno pokazuje u tom kontekstu da ispitanik prihvaća predloženu obradu svojih osobnih podataka. Štunja, unaprijed kvačicom označeno polje ili manjak aktivnosti stoga se ne bi smjeli smatrati privolom.

Dalje, privola bi trebala obuhvatiti sve aktivnosti obrade koje se obavljaju u istu svrhu ili svrhe. Kada obrada ima višestruke svrhe, privolu bi trebalo dati za sve njih. Ako se privola ispitanika treba dati nakon zahtjeva upućenog elektroničkim putem, taj zahtjev mora biti jasan, jezgrovit i ne smije nepotrebno ometati upotrebu usluge za koju se upotrebljava.

Također, 42. Uvodnom izjavom Preambule propisano je da bi, ako se obrada temelji na privoli ispitanika, voditelj obrade trebao moći dokazati da je ispitanik dao privolu za postupak obrade. Zaštitnim mjerama, posebno u kontekstu pisane izjave o drugom pitanju, trebalo bi se osigurati da je ispitanik svjestan činjenice da daje privolu i do koje mjere se ona daje. U skladu s Direktivom Vijeća 93/13/EEZ o nepoštenim uvjetima u potrošačkim ugovorima, izjavu o privoli koju je unaprijed sastavio voditelj obrade trebalo bi ponuditi u razumljivom i lako dostupnom obliku, uz upotrebu jasnog i jednostavnog jezika te u njoj ne bi smjelo biti nepoštenih uvjeta. Da bi ispitanik mogao dati privolu informiran, trebao bi barem znati identitet voditelja obrade i svrhe obrade za koju se upotrebljavaju osobni podaci. Ne može se smatrati da je privola dana dobrovoljno ako ispitanik nema istinski ili slobodan izbor ili ako nije u mogućnosti odbiti ili povući privolu bez posljedica.

U mišljenju br. 249 o obradi podataka na radnome mjestu, Radna skupina za zaštitu podataka iz članka 29. Direktive 95/46/EZ iznosi mišljenje da se vrlo vjerojatno privola ne može smatrati zakonitim pravnim temeljem za obradu osobnih podataka zaposlenika ili potencijalnih zaposlenika, osim ako isti mogu obradu odbiti bez štetnih posljedica.

Naime, zaposlenici su rijetko u situaciji da slobodno daju, odbiju ili povuku privolu s obzirom na ovisnost koja proizlazi iz odnosa između poslodavca i zaposlenika. Osim u iznimnim situacijama, poslodavci će se morati oslanjati na neku drugu pravnu osnovu koja nije privola, kao što je potreba za obradom podataka u svrhe njihova legitimnog interesa. Međutim, legitimni interes sam po sebi nije dovoljan da bi imao prednost pred pravima i slobodama zaposlenika. Legitimni interes poslodavca može biti pravna osnova za obradu osobnih podataka zaposlenika samo ako je obrada podataka nužna za zakonitu svrhu i u skladu je s načelima proporcionalnosti i supsidijarnosti.

Dalje tumačimo legitimni interes kao mogući pravni temelj za obradu osobnih podataka zaposlenika.

Uvodna izjava 47 Opće Uredbe propisuje da legitimni interesi voditelja obrade, među ostalim onih interesa voditelja obrade kojem se osobni podaci mogu otkriti ili treće strane, mogu predstavljati pravnu osnovu za obradu pod uvjetom da interesi ili temeljna prava i slobode ispitanika nemaju prednost, uzimajući u obzir razumna očekivanja ispitanika koja se temelje na njihovom odnosu s voditeljem obrade. Takav legitiman interes mogao bi na primjer postojati u slučaju relevantnog i odgovarajućeg odnosa ispitanika i voditelja obrade u situacijama poput one kada je ispitanik klijent voditelja obrade ili u njegovoj službi. U svakom slučaju postojanje legitimnog interesa zahtijevalo bi pažljivu procjenu, među ostalim i toga može li ispitanik u vrijeme i u kontekstu prikupljanja osobnih podataka razumno očekivati obradu u dotičnu svrhu. Interesi i temeljna prava ispitanika posebno bi mogli nadvladati interes voditelja obrade ako se osobni podaci obrađuju u okolnostima u kojima ispitanici razumno ne očekuju daljnju obradu. Može se smatrati da postoji legitiman interes kod obrade osobnih podataka provedene za potrebe izravnog marketinga.

Neovisno o pravnoj osnovi za obradu podataka, prije početka obrade trebalo bi ispitati proporcionalnost kako bi se razmotrilo je li obrada potrebna radi ostvarenja zakonite svrhe te koje se mjere moraju poduzeti kako bi se osiguralo da su kršenja prava na privatni život i tajnost komunikacija svedena na najmanju moguću mjeru. To bi mogao biti dio procjene učinka na zaštitu podataka.

Poduzeća sve češće dostavljaju svojim klijentima podatke o zaposlenicima kako bi osigurala pouzdano pružanje usluga. Ti podaci mogu biti prilično pretjerani ovisno o opsegu usluga koje se pružaju (npr. mogu uključivati i fotografiju zaposlenika). Međutim, zbog neravnoteže moći, kao što je *supra* već pojašnjeno, zaposlenici nisu u mogućnosti dobrovoljno dati privolu na obradu svojih osobnih podataka koju provodi poslodavac, a ako obrada podataka nije proporcionalna, poslodavac nema pravnu osnovu za nju.

Ukoliko voditelj obrade utvrdi da ima legitiman interes za slanje životopisa svojih zaposlenika svojim potencijalnim klijentima, od odlučujuće je važnosti da se radi samo o onim osobnim podacima zaposlenika koji su bili odlučujući za zapošljavanje upravo te osobe. Znači, treba se raditi samo o onim podacima koji se odnose na njegova stručna znanja, formalno obrazovanje, odlučujuće poslovno iskustvo, a nikako o podacima koji nisu odlučujući za stručno izvršenje određenog zadatka. Primjerice, ne bi se smjele prosljeđivati fotografija niti privatna adresa.

Ujedno, člankom 29., stavkom 1. Zakona o radu (NN 93/14 i 127/17) je propisano da se osobni podaci radnika smiju prikupljati, obrađivati, koristiti i dostavljati trećim osobama samo ako je to određeno ovim ili drugim zakonom ili ako je to potrebno radi ostvarivanja prava i obveza iz radnog odnosa, odnosno u vezi s radnim odnosom.

Nadalje, člankom 29., stavkom 2. istoga Zakona je određeno da ako je osobne podatke iz stavka 1. ovoga članka potrebno prikupljati, obrađivati, koristiti ili dostavljati trećim osobama radi

ostvarivanja prava i obveza iz radnoga odnosa, odnosno u vezi s radnim odnosom, poslodavac mora unaprijed pravilnikom o radu odrediti koje će podatke u tu svrhu prikupljati, obrađivati, koristiti ili dostavljati trećim osobama.

Svaki međunarodni prijenos podataka o zaposlenicima voditelju obrade u trećoj zemlji izvan EU trebao bi se odvijati samo ako ta zemlja osigurava odgovarajuću razinu zaštite. Koja god bila osnova za prijenos, on treba biti u skladu s odredbama Opće uredbe o zaštiti podataka.

Prijenos je moguć na temelju Komisijine odluke o primjerenosti razini zaštite u trećoj zemlji. Nadalje, prijenos je moguć ako podliježe odgovarajućim zaštitnim mjerama, kao što su standardne ugovorne klauzule ili obvezujuća korporativna pravila. Također, prijenos je moguć u posebnim situacijama iz članka 49. Opće uredbe.

Ukoliko ne postoji odluka o primjerenosti, nema odgovarajućih zaštitnih mjera, uključujući obvezujuća korporativna pravila, i kad nije primjenjivo nijedno odstupanje za posebne situacije, prijenos u treću zemlju može se ostvariti samo ako se prijenos ne ponavlja, ako se odnosi samo na ograničen broj ispitanika, nužan je za potrebe uvjerljivih, legitimnih interesa voditelja obrade koji nisu podređeni interesima ili pravima i slobodama ispitanika, a voditelj obrade procijenio sve okolnosti prijenosa podataka te je na temelju te procjene predvidio odgovarajuće zaštitne mjere u pogledu zaštite osobnih podataka. Voditelj obrade obavješćuje nadzorno tijelo o tom prijenosu. Uz pružanje informacija iz članaka 13. i 14., voditelj obrade ispitanika obavješćuje o prijenosu i o uvjerljivim legitimnim interesima.

POSTUPANJE PO PRITUŽBAMA / ZAHTJEVIMA ZA UTVRĐIVANJE POVREDE PRAVA - Provođenje upravnog postupka

PRIKAZ NEKOLIKO PRIMJERA IZ PRAKSE

Primjer 1. – Objava osobnih podataka na Facebook profilu

Agencija postupala je po zahtjevu za utvrđenje prava na zaštitu osobnih podataka podnositelja u kojemu se, između ostalog, navodi kako je podnositelj pokrenuo poseban postupak u svrhu zaštite svojih prava (tužbu) protiv donesenog akta od strane poslodavca (općine) kao tijela javne vlasti pred nadležnim sudom. Navedeni postupak odnosio se na ostvarivanje njegovih prava iz radnog odnosa. Podnositelj zahtjeva je naveo da je njegov poslodavac na svojem službenom *Facebook* profilu javno objavio akt (tužbu) kojim je podnositelj zahtjeva zatražio preispitivanje svojih prava, a koji u sebi sadrži njegove osobne podatke u sljedećem opsegu: ime i prezime i privatnu adresu. Navedenim postupanjem njegovi osobni podaci (ime i prezime i privatna adresa) postali su javni i dostupni neograničenom broj primatelja i posjetitelja Facebook stranice tijela javne vlasti i

izvrgnuti svakojakim negativnim komentarima posjetitelja te stranice koji definitivno štete njegovoj časti i ugledu.

Agencija je provela postupak sukladno svojim ovlastima te donijela rješenje kojim je zahtjev ocijenila osnovanim zbog nepostojanja zakonite osnove za javnu objavu osobnih podataka osobito podataka o privatnoj adresi.

Predmetnim rješenjem Agencija je donijela korektivnu mjeru odnosno naložila brisanje osobnih podataka podnositelja zahtjeva budući da je utvrđeno kako su objavljeni bez postojanja zakonite osnove, te zabranila svako daljnje objavljivanje osobnih podataka podnositelja zahtjeva kao i drugih fizičkih osoba na društvenoj mreži Facebook bez pravnog temelja i zakonite svrhe.

Agencija je kao odlučnu činjenicu za donošenje svoje odluke uzela u obzir i odredbe posebnog zakona (Zakona o pravu na pristup informacijama) te utvrdila da se odredbe tog Zakona ne primjenjuju na stranke u sudskim, upravnim i drugim na zakonu utemeljenim postupcima, kojima je dostupnost informacija iz tih postupaka utvrđena propisom.

Isto tako u skladu s obvezom iz članka 18. Zakona o zaštiti osobnih podataka općini je naloženo poduzimanje odgovarajućih tehničkih i organizacijskih mjera kako bi osobni podaci bili odgovarajuće zaštićeni od neovlaštenih pristupa, objave i svih drugih neovlaštenih raspolaganja istima.

Primjer 2. – Neovlašteno raspolaganje osobnim podacima

Agencija za zaštitu osobnih podataka postupala je po zahtjevu za utvrđivanje povrede prava podnositelja u kojemu se navodi da su mu povrijeđena njegova prava na način da je zaposlenik Poreznog tijela upotrijebio njegove osobne podatke (OIB i privatnu adresu) bez njegove suglasnosti i to u postupku u kojem njegovi osobni podaci nisu bili bitni niti potrebni. U zahtjevu podnositelj također navodi kako je navedenim radnjama zaposlenik Poreznog tijela zlorabio svoje ovlasti.

Postupajući po predmetnom zahtjevu Agencija je provela postupak sukladno svojim ovlastima te donijela rješenje kojim je ocijenila zahtjev osnovanim, odnosno utvrdila povredu prava na zaštitu osobnih podataka.

Rješenjem je naložila mjere koje se odnose na poreznog službenika u vidu zabrane svakog daljnjeg korištenja i raspolaganja sa osobnim podacima podnositelja zahtjeva bez postojanja zakonite svrhe i pravnog temelja.

U konkretnom slučaju Agencija nije utvrdila nezakonito postupanje poreznog tijela već da je u pitanju ljudski faktor (nepoštivanja zakona i internih akata od strane poreznog službenika koji je u obavljanju poslova i zadaća postupao protivno pozitivnim propisima i etičkim načelima službe, a time naštetio ugledu poslodavca odnosno službe u kojoj radi).

Utvrđeno je kako porezno tijelo postupa u skladu s propisima o zaštiti osobnih podataka (donijelo je interne akte, poduzima odgovarajuće mjere zaštite kako bi se osobni podaci koje obrađuje predmetni voditelj zbirke osobnih podataka putem informacijskog sustava (ISPU) zaštitili od slučajne gubitka ili uništenja od nedopuštenog pristupa, nedopuštene promjene i svake druge zlorabuse, utvrđeno je da djelatnici imaju dodijeljena ovlaštenja za pristup informacijskom sustavu te da su sa svojim pravima i obvezama u odnosu na zaštitu osobnih podataka upoznati internim aktima).

Primjer 3. – Objava osobnih podataka o zdravlju

Agencija za zaštitu osobnih podataka postupala je po zahtjevu za utvrđivanje povrede prava na zaštitu osobnih podataka podnositelja zahtjeva vezano uz obradu njegovih osobnih podataka od strane zdravstvene ustanove.

U predmetnom zahtjevu za utvrđivanje povrede prava na zaštitu osobnih podataka se navodi kako je zaposlenik zdravstvene ustanove (predstojnik Klinike) dao intervju, a potom i izdao priopćenje, u kojem je iznosio podatke o zdravstvenom stanju podnositelja zahtjeva, detaljno pojašnjavajući njegovo viđenje zdravstvenog stanja i provedene medicinske postupke nad podnositeljem zahtjeva, zlorabeći na taj način povjerenje pacijenta koji se zdravstvenoj ustanovi obratio za pomoć, pri tome pokušavajući omalovažiti i difimirati podnositelja, ali i druge pacijente.

Agencija je provela postupak te u granicama svojih ovlasti donijela rješenje kojim je zahtjev ocijenjen osnovanim. Utvrđeno je da je obradom osobnih podataka o zdravlju protivno prvotnoj svrsi u koju su prikupljeni njegovi osobni podaci, odnosno bez postojanja uvjeta za zakonitu obradu (iznošenje) osobnih podataka i poduzimanja odgovarajućih tehničkih i organizacijskih mjera zaštite došlo do povrede odredbi Opće uredbe o zaštiti podataka, kao i odredbe posebnih propisa koji liječnike obvezuju na čuvanje liječničke tajne (Zakon o liječništvu, Zakon o zaštiti prava pacijenata), zbog čega je narušena privatnost podnositelja zahtjeva.

Rješenjem su zdravstvenoj ustanovi kao voditelju obrade naložene korektivne mjere u vidu poduzimanje odgovarajućih tehničkih i organizacijskih mjera zaštite osobnih podataka pacijenata, kako bi se osigurala odgovarajuća razina sigurnosti i povjerljivosti u obradi osobnih podataka, odnosno kako bi se osobni podaci pacijenata zaštitili od neovlaštenog otkrivanja i drugih mogućih zlouporaba.

Primjer 4. – Pravo uvida u osobne podatke

Agencija za zaštitu osobnih podataka postupala je po zahtjevu za utvrđivanje povrede prava u kojem podnositelj navodi kako je zatražio pristup osobnim podacima i informacijama odnosno dostavljanje potvrde o obradi njegovih osobnih podataka od strane poslodavca. Između ostalog podnositelj zahtjeva zatražio je dostavljanje informacija o obradi njegovih osobnih podataka od strane službenika za zaštitu osobnih podataka.

Agencija je provela postupak te u granicama svojih ovlasti donijela rješenje kojim je zahtjev ocijenjen djelomično osnovanim iz razloga što nije utvrđeno da su pružene sve informacije i dano obrazloženje o obradi njegovih osobnih podataka na način kako to nalažu odredbe Opće uredbe o zaštiti podataka. Utvrđeno je da nije odobren pristup osobnim podacima i nisu pružene informacije o svrsi obrade njegovih osobnih podataka, pravnom temelju, kategorijama osobnih podataka, primateljima, razdoblju pohrane, pravu na brisanje, ispravak ili ograničenje obrade, podnošenje pritužbe nadzornom tijelu.

Navedenom zahtjevu podnositelja bivši poslodavac nije udovoljio u cijelosti. Razvidno da su podnositelju zahtjeva pružene samo određene informacije, ali ne sve kako to nalažu odredbe Opće uredbe o zaštiti podataka. Neovisno o tome što podnositelj zahtjeva više nije zaposlenik kod poslodavca kao voditelja obrade, poslodavac obrađuje i čuva njegove podatke kako to propisuju

posebni zakoni te je obveza voditelja obrade da postupi po zahtjevu ispitanika i da mu dade sve informacije o obradi njegovih osobnih podataka.

Međutim, Općom uredbom o zaštiti podataka nije regulirana obveza službenika o zaštiti osobnih podataka da potpisuje tj. donosi akt kojim se odlučuje o zahtjevu/pravu ispitanika jer je sukladno Općoj uredbi o zaštiti podataka za ne postupanje u skladu i po odredbama Opće uredbe o zaštiti podataka odgovoran voditelj obrade, a ne službenik za zaštitu osobnih podataka kod voditelja obrade te je iz tih razloga zahtjev podnositelja u tom dijelu odbijen kao neosnovan.

Primjer 5. – Postavljanje videonadzornih kamera u stambenim zgradama

Agencija za zaštitu osobnih podataka zaprimila je zahtjev za utvrđivanje povrede prava na zaštitu osobnih podataka pojedinih suvlasnika stambene zgrade u kojem isti navode kako je jedan od suvlasnika stambene zgrade postavio videonadzornu kameru na stubištu, iznad ulaznih vrata u stan, a koja prema navodima istih snima prostor ulaznih vrata u stambenu zgradu te stepenište stana. S tim u vezi isti navode kako svi suvlasnici stambene zgrade koriste navedene prostore. Također u zahtjevu za zaštitu prava navodi se kako je videonadzorna kamera postavljena bez prethodne obavijesti o postavljenju istih, odnosno kako nije održan sastanak/skup stanara, a tako niti tražena privola suvlasnika stambene zgrade za postavljanje videonadzornog sustava.

Ova Agencija je sukladno svojim zakonskim ovlastima provela postupak te donijela rješenje kojim je ocijenila zahtjev neosnovanim iz razloga što je utvrđeno da se ne radi o obradi osobnih podataka.

Utvrđeno je kako navedeni uređaj nije spojen na električno napajanje te iako postavljeni uređaj nalikuje na kameru ne prikuplja i ne obrađuje osobne podatke u smislu odredbi Opće uredbe o zaštiti podataka i Zakona o provedbi opće uredbe o zaštiti podataka. Navedenom svjedoči i činjenica kako ne postoji uređaj za pohranu snimki, a time ni do izvršavanja radnji na osobnim podacima (snimanja).

Primjer 6. - Zloupotreba identiteta u telekomunikacijskom sektoru

Agencija za zaštitu osobnih podataka je zaprimila zahtjev za utvrđivanje povrede prava na zaštitu osobnih podataka podnositelja, a vezano za obradu njegovih osobnih podataka od strane teleoperatora. Podnositelj zahtjeva tvrdi kako nije sklopio ugovore o pružanju usluge s navedenim društvom, niti je zatražio kupnju mobilnog uređaja na njegovu nevažeću osobnu iskaznicu.

Agencija je provela postupak u granicama svojih ovlasti i donijela rješenje kojim je zahtjev za utvrđivanje povrede prava na zaštitu osobnih podataka ocijenila osnovanim i izrekla kondemnatornu mjeru zabrane daljnje obrade osobnih podataka podnositelja u svrhu prava i obveza koja proizlaze iz spornog ugovornog odnosa.

U cjelokupno provedenom postupku utvrđeno je kako teleoperator prilikom obrade osobnih podataka nije utvrdio identitet osobe koja je sklopila pretplatnički ugovor za telefonski broj budući da su nadzornim aktivnostima utvrđene nesukladnosti u djelu osobnih podataka koji se odnose na podnositelja zahtjeva. Utvrđeno je kako zahtjev za zasnivanje pretplatničkog odnosa sadrži različite podatke od osobnih podataka sadržanih u osobnoj iskaznici koja je priložena uz zahtjev za

utvrđivanje povrede prava, točnije sadrži broj osobne iskaznice koja je prema navodima podnositelja zahtjeva ukradena, te u vrijeme sklapanja pretplatničkog ugovora ista nije bila važeća.

Primjer 7. - Obrada osobnih podataka od strane agencija za naplatu potraživanja

Agencija je zaprimila zahtjev za utvrđivanje povrede prava na zaštitu osobnih podataka podnositelja zahtjeva u kojem se navodi kako je zaprimio telefonski poziv na privatni broj svog mobilnog telefona od strane društva za naplatu potraživanja te da ju je u tom razgovoru zaposlenik agencije za naplatu potraživanja zatražio da svojoj susjedi prenese poruku da isti imaju poruku za nju. Nadalje ista navodi kako su nakon toga uslijedila pitanja vezana za njezinu susjedu. Naposljetku podnositelj zahtjeva navodi kako nema dugovanja prema trećim osobama, a tako niti obveze prema agenciji za naplatu potraživanja.

Nakon provedenog ispitnog postupka te utvrđenog činjeničnog stanja ova Agencija je cijenila zahtjev osnovanim i donijela rješenje i izrekla kondemnatornu mjeru zabrane obrade osobnih podataka podnositelja zahtjeva od strane agencije za naplatu potraživanja.

U postupku je utvrđeno kako je podnositelj zahtjeva uistinu telefonski kontaktiran od strane jedne agencije za naplatu potraživanja bez postojanja zakonite svrhe i pravne osnove a vezano za dugovanje njegove susjede. Dakle, djelatnik društva stupio u kontakt sa podnositeljem zahtjeva, nakon što isti nije mogao doći do informacije o kontakt podacima njegove susjede putem javnih registara.

Imajući u vidu kako je u konkretnom slučaju došlo do nezakonite obrade osobnih podataka podnositelja zahtjeva, točnije do neovlaštenog otkrivanja osobnih podataka o trećoj osobi/dužniku Agencija je ujedno dala i preporuku/uputu za unapređenje zaštite osobnih podataka te navedeno društvo upozorila na potrebu zaštite osobnih podataka u punom opsegu kadrovskih, organizacijskih i tehničkih mjera zaštite, sukladno članku 18. Zakona o zaštiti osobnih podataka sve kako ne bi dolazilo do zlouporabe osobnih podataka. Također, navedenom društvu je ukazano na obvezu poduzimanja kadrovskih mjera zaštite kako osobni podaci klijenata ne bi bili dostupni neovlaštenim osobama, a što bi, između ostalog, značilo da prilikom upućivanja telefonskih poziva/telefonske komunikacije djelatnici društva ne smiju razotkrivati osobne podatke treće osobe, odnosno prilikom komunikacije s klijentima prvenstveno su obvezni nedvojbeno utvrditi njihov identitet.

Dana je uputa da je agencija za naplatu potraživanja dužna osobne podatke obrađivati na pošten i zakonit način i donijeti interne politike i procedure vezane za postupanje sa osobnim podacima te da utvrdi tko sve i kojim podacima ima pristup, kao i da se osobe koje imaju pristup podacima obvežu na čuvanje tajnosti podataka, odnosno da potpišu izjavu o povjerljivosti.

Osim gore navedene preporuke/upute za postupanje glede zaštite osobnih podataka ova Agencija je navedenom društvu zabranila se svaku daljnju obradu osobnih podataka podnositeljice zahtjeva bez postojanja zakonite osnove, a tako i svako daljnje kontaktiranje osoba za koje nisu pribavljeni relevantni dokazi da su stvarni dužnici.

Primjer 8. – Objava osobnih podataka po Zakonu o pravu na pristup informacijama

Agencija za zaštitu osobnih podataka postupala je po zahtjevu za utvrđivanje povrede prava na zaštitu osobnih podataka podnositelja vezano za objavu dokumenata koji su objavljeni sukladno Zakonu o pravu na pristup informacijama te su na taj način postali javno dostupni, a potom objavljeni i na Internetu. Sporni dokumenti se odnose na transparentnost trošenja proračunskih sredstava jedne zdravstvene ustanove, a podnositelj navodi da se dokumenti odnose na točno određene osobe, konkretno da je objavljeno više dokumenata koji se odnose na njegovu plaću, školovanje i putne troškove. Navedeni dokumenti postali su dostupni javnosti temeljem zahtjeva za pravo na pristup informacijama.

Agencija je sukladno ovlastima ocijenila zahtjev neosnovanim i donijela rješenje kojim se zahtjev podnositelja odbija. U provedenom postupku je utvrđeno da su na internetskoj stranici objavljeni podaci koji se, između ostaloga, odnose na zdravstvenu ustanovu, kao tijelo javne vlasti te da su objavljeni dokumenti koji sadrže osobne podatke koji se odnose na podnositelja zahtjeva. Naime, uvidom u sadržaj predmetne stranice utvrđeno je da ista, između ostaloga, sadrži dokumente koji se odnose na bruto plaću, putne troškove i školovanje tj. osobne podatke podnositelja zahtjeva. Iz dokumenta koji su objavljeni razvidno je da su isti dobiveni u svrhu poštivanja pravnih obveza koje proizlaze iz Zakona o pravu na pristup informacijama koji propisuje da su informacije dostupne svakoj domaćoj ili stranoj fizičkoj i pravnoj osobi u skladu s uvjetima i ograničenjima reguliranim navedenim Zakonom. U opisanom slučaju utvrđeno je da su informacije točnije dokumenti koji sadrže osobne podatke dobiveni temeljem Zakona o pravu na pristup informacijama te da su poštivane sve odredbe navedenog posebnog zakona, posebice one koje se odnose na ograničenja odnosno zaštitu osobnih podataka. U ovoj upravnoj stvari kao odlučna činjenica, cijenjeno je da se radi o dva ustavom zajamčena prava (pravo na zaštitu osobnih podataka i pravu na pristup/dostupnost informacijama) da navedena prava nisu apsolutna, već je za ostvarivanje pojedinog od tih dvaju prava potrebno od slučaja do slučaja utvrditi pravičnu ravnotežu/balans. Obzirom na utvrđene činjenice i dokumentaciju koja je objavljena utvrđeno je kako na obradu osobnih podataka u navedenom opsegu prevladava pravo na pristup informacijama, odnosno prevladava interes javnosti u odnosu na zaštitu osobnih podataka (javno dostupne informacije). S obzirom na to da je pravni temelj za obradu osobnih podataka u konkretnom slučaju Zakon o pravu na pristup informacija koji ujedno propisuje da korisnik koji raspolaže informacijom ima pravo tu informaciju javno iznositi isto je i Općoj uredbi o zaštiti podataka jer za prikupljanje i daljinu obradu pravni temelj nalazimo u poštovanju pravnih obveza voditelja obrade. Isto tako, utvrđeno je da je prilikom obrade osobnih podataka poštovano načelo razmjernosti i smanjenja količine podataka, a time i javnosti omogućena dostupnost osobnih podataka u nužnom opsegu.

PROVOĐENJE POSTUPKA PO SLUŽBENOJ DUŽNOSTI

Primjer 1. – Objava podataka u klasičnim (tiskanom izdanju) i digitalnim medijima

Agencija za zaštitu osobnih podataka je zaprimila predstavke Vlade Republike Hrvatske, Ureda za ljudska prava i prava nacionalnih manjina, Ministarstva unutarnjih poslova i Agencije za elektroničke medije vezane uz objavu osobnih podataka žrtve trgovanja ljudima, kao i podataka o članovima njegove obitelji u tiskanom izdanju i na internetskim stranicama određenog medija.

Postupajući po predmetnom zahtjevu Agencija je provela postupak sukladno svojim ovlastima te donijela rješenje kojim je primjenom načela razmjernosti utvrdila povredu prava na zaštitu podataka.

Iako se medij očitovao da namjera predmetnih tekstova objavljenih u tiskanom izdanju te na portalu nije bila razotkrivanje identiteta žrtve kaznenih djela niti povreda prava pripadnika nacionalnih manjina, već ukazivanje na probleme i manjkavost sustava kada se radi o slučajevima trgovanja ljudima, s obzirom da se jako malo takvih slučajeva sudski procesuiraju, u postupku je utvrđeno da u konkretnom slučaju prevladava pravo na zaštitu osobnih podataka u odnosu na pravo na informiranje javnosti, te da se objavom članka grubo krše prava žrtve na zaštitu njezina identiteta, osobito što je objavljen članak u kojemu su učinjene javno dostupne fotografije i anamneza o zdravstvenom stanju žrtve.

U konkretnom slučaju Agencija je uzela u obzir i primjenu je Zakon o medijima kao poseban zakon, kojim se, između ostalog, uređuju pretpostavke za ostvarivanje načela slobode medija, prava novinara i drugih sudionika u javnom informiranju na slobodu izvješćivanja i dostupnost javnim informacijama, prava i obveze nakladnika, ostvarivanje prava na ispravak i odgovor. Međutim i prema Zakonu o medijima mediji su dužni poštovati pravo na zaštitu identiteta svjedoka i oštećenika kaznenih djela i bez njihovog znanja i pristanka ne smiju otkriti njihov identitet.

U tijeku postupka je utvrđeno da su sporni članci uklonjeni sa internetskih stranica medija te nisu više nisu javno dostupni izravnim pristupom.

Agencija za zaštitu osobnih podataka ne spori pravo medijima da informiraju javnost o određenim događajima (u ovom slučaju o mogućem počinjenju kaznenog djela trgovanja ljudima). Međutim, informiranje javnosti u konkretnom slučaju moglo se postići i manje invazivnom metodom, na način da se zaštiti identitet žrtve u postupku, a osobito da se ne objavljuju uznemirujuće fotografije kao i anamneza i status koji su sebi sadrži nerazmjerno velik opseg osobnih podataka o zdravlju. Osobito bitno je istaknuti kako osobni podaci o zdravlju po svojoj naravi spadaju u posebno osjetljive osobne podatke koji se mogu prikupljati i obrađivati samo iznimno i za koje je propisano poduzimanje posebnih mjera tehničke zaštite budući da njihovom obradom osobito obznamljivanjem u javnosti može doći do povrede temeljnih prava i sloboda pojedinca.

U ovoj upravnoj stvari utvrđeno je da je objava osobnih podataka žrtve kaznenog djela u spornim člancima prekomjerna svrha za koju su isti bili objavljeni, osobito cijeneći činjenicu koju ističe nakladnik da svrha članaka nije bila otkrivanje identiteta žrtve kaznenih djela nego ukazivanje na probleme i manjkavost sustava kada se radi o slučajevima trgovanja ljudima.

Primjer 2. – Videonadzor u školskoj ustanovi

Agencija za zaštitu osobnih podataka postupajući po službenoj dužnosti provela je nadzor nad obradom osobnih podataka putem video nadzornog sustava u školskoj ustanovi. U ovoj upravnoj stvari utvrđeno je da za obradu osobnih podataka (snimanje računalnih učionica video nadzornim sustavom) ne postoji zakonita (opravdana) svrha niti pravni temelj pa je takva obrada osobnih

podataka nepoštena i nezakonita, odnosno protivna Zakona o zaštiti osobnih podataka. Snimanjem učionica u kojima borave učenici za vrijeme nastave i nastavno osoblje škole snimaju unutarnji prostori (a ne ulazi/izlazi u radne prostorije) u kojima se odvija nastava i u kojima boravi nastavno osoblje kao i sami učenici dolazi do cjelodnevnog praćenja učenika i nastavnika snimanje video nadzornim kamerama predstavlja prilično invazivnu metodu prikupljanja i obrade osobnih podataka učenika i nastavnog osoblja te kako bi se svrha zbog koje je uspostavljen video nadzorni sustav u računalnim učionicama mogla postići drugim, manje invazivnim metodama i na način da se snimanje ne vrši u samim računalnim učionicama, već na drugim mjestima i prostorima na kojima je takvo snimanje dopušteno u smislu odredbi Zakona o zaštiti na radu (NN, 118/14, 154/14, 94/18, 96/18)..

Ovakvom invazivnom metodom obrade osobnih podataka došlo je do narušavanja privatnosti tijekom nastave i učenja kako učenika tako i nastavnog osoblja na radnom mjestu što je protivno odredbama Zakona o zaštiti na radu, naročito iz razloga što nije pribavljena prethodna suglasnost Radničkog vijeća kao ni privola svakog pojedinog punoljetnog učenika, odnosno svakog pojedinog roditelja/zakonskog zastupnika maloljetnog učenika koje bi se smatrale zakonitom osnovom za obradu.

Također, treba uzeti u obzir da se navedenim snimanjem obrađuje veliki opseg osobnih podataka velikog broja osoba (nastavnog osoblja te učenika škole, od kojih su većina maloljetne osobe, te kao takvi predstavljaju najranjiviju kategoriju osoba čiji se osobni podaci obrađuju). Škola, kao voditelj zbirke osobnih podataka koja sukladno svojim zakonskim ovlastima, prikuplja i obrađuje veliki opseg osobnih podataka, naročito osobnih podataka učenika/maloljetnih osoba treba biti svjesna i voditi računa o tome da djeca zaslužuju posebnu zaštitu u pogledu svojih osobnih podataka, budući mogu biti manje svjesna rizika, posljedica i zaštitnih mjera te svojih prava u vezi s obradom osobnih podataka.

Osim toga, treba voditi računa da snimanje predmetnim video nadzornim sustavom može imati dalekosežne posljedice na razvoj učenika i njegov integritet, te se može negativno odraziti na njegovu koncentraciju i učenje, što predstavlja dodatne razloge da se na druge, manje invazivne načine ostvari sigurnost učenika.

Istoj školi zabranjena je obrada osobnih podataka učenika i nastavnika na način da se za čitavo vrijeme nastave video nadzornim kamerama u računalnim učionicama škole snimaju učenici i nastavnici te je naloženo brisanje svih video zapisa nastalih snimanjem video nadzornim kamerama u računalnim učionicama škole, a koji su prikupljeni bez pravne osnove.

UPRAVNI SPOROVI U 2018.

Primjer 1. – Objava osobnih podataka u medijima

Agencija za zaštitu osobnih podataka rješavala je zahtjev za utvrđivanje povrede prava na zaštitu osobnih podataka podnositelja zahtjeva vezano uz objavu članka na portalu i u tiskanom izdanju tjednika te na web portalu objavljen članak pod senzacionalističkim naslovom uz navođenje imena i prezimena i fotografija čime je istu nesporno moguće identificirati te povezati sa svim neistinitim napisima u navedenom članku, a članak je javno dostupan upisivanjem imena i prezimena podnositelja u tražilicu *Google*.

U ovom predmetu doneseno je rješenje kojim je zahtjev ocijenjen osnovanim, utvrđeno je da je došlo do povrede prava na zaštitu osobnih podataka te je naloženo brisanje/uklanjanje predmetne poveznice (URL-a) kao rezultat pretraživanja.

Navedeno društvo podnijelo je upravnu tužbu protiv rješenja Agencije sukladno Zakonu o upravnim sporovima. Postupak po tužbi je u tijeku.

Primjer 2. – Objava osobnih podataka u medijima

Agencija za zaštitu osobnih podataka rješavala je zahtjev za utvrđivanje povrede prava podnositelja koji se pritužuje da mu je povrijeđeno njegovo pravo na zaštitu osobnih podataka objavom njegovog imena i prezimena i osobnog identifikacijskog broja u novinskom članku tjednih novina.

Sukladno svojim ovlastima Agencija je provela postupak i donijela rješenje kojim je odbila zahtjev kao neosnovan odnosno cijenila je da objavu osobnih podataka podnositelja zahtjeva treba promatrati sa gledišta uloge i funkcije koju obavlja kao samostalnu djelatnost podaci vezani uz njegov profesionalni život/rad, a u tom kontekstu spominju se i njegovi osobni podaci u navedenom članku, kao sastavni dio temeljnih podataka vezanih uz njegovu profesiju. Također je cijenjena okolnost da su osobni podaci podnositelja objavljeni i na drugim javno dostupnim stranicama, a time i javno dostupni bez dokazivanja pravnog interesa.

Podnositelj zahtjeva podnio je upravnu tužbu i zatražio preispitivanje pobijanog rješenja pred nadležnim upravnim sudom, upravni spor je u tijeku.

Primjer 3. Obrada osobnih podataka videonadzorom

Agencija za zaštitu osobnih podataka rješavala je zahtjev za zaštitu prava vezano uz videonadzor dvorišta javne površine/ceste kojima se koriste podnositelji zahtjeva u izvršavanju prava suvlasništva.

U ovom predmetu doneseno je rješenje kojim je zahtjev ocijenjen osnovanim te je utvrđeno da je došlo do povrede prava podnositelja zahtjeva i protivnoj stranci zabranjeno snimanje navedenog prostora. Također je protivnoj stranci naloženo brisanje svih zapisa nastalih snimanjem navedenog prostora. Nezadovoljna rješenjem stranka podnijela tužbu je nadležnom upravnom sudu iz razloga što smatra da ima pravo videonadzorom snimati navedeni prostor.

Upravni spor je u tijeku.

Primjer 4. – Obrada osobnih podataka videonadzorom u zajedničkim prostorijama suvlasnika

Agencija za zaštitu osobnih podataka rješavala je zahtjev za zaštitu prava vezano uz postavljene videonadzor u zajedničkim prostorijama svih suvlasnika zgrade kojim se obrađuju njihovi osobni podaci.

U ovom predmetu doneseno je rješenje kojim su zahtjevi podnositelja ocijenjeni osnovanim te je protivnoj stranci zabranjeno snimanje (prikupljanje i pohranjivanje osobnih podataka suvlasnika) budući da za takvo postupanje nije utvrđeno postojanje zakonite osnove (privole svih suvlasnika).

Nezadovoljan ovakvim rješenjem predstavnik suvlasnika kao protivna strana podnio tužbu je nadležnom upravnom sudu iz razloga što smatra da ima pravo videonadzorom snimati navedeni prostor. Upravni spor je u tijeku.

Primjer 5. – Prosljeđivanje osobnih podataka radnika drugim primateljima

Agencija za zaštitu osobnih podataka rješavala je zahtjev za utvrđivanje povrede prava koji se odnosio na prosljeđivanje osobnih podataka podnositelja od strane poslodavca drugim primateljima.

U ovom predmetu doneseno je rješenje kojim je zahtjev ocijenjen osnovanim, utvrđeno je da je došlo do povrede prava podnositelja zahtjeva te je poslodavcu naloženo poduzimanje odgovarajućih mjera zaštite, te da vodi brigu o opsegu osobnih podataka koji se dostavljaju na korištenje.

Nezadovoljna stranka/poslodavac podnijela je tužbu pred nadležnim upravnim sudom iz razloga što smatra da nije obrađivao osobne podatke u svojstvu voditelja obrade već kao stranka u drugom (posebnom) postupku u obrani svoje stranačke pozicije. Upravni spor je u tijeku.

Primjer 6. – Pravo pristupa/uvida u osobne podatke

Agencija za zaštitu osobnih podataka rješavala je zahtjev za zaštitu prava podnositelja vezano uz ostvarivanje prava uvida u osobne podatke kod voditelja obrade (tijelo javne vlasti).

U ovom predmetu doneseno je rješenje kojim je zahtjev odbijen kao neosnovan. Ocijenjeno je kako je podnositelj zahtjeva već ostvario svoja prava te nije bilo razloga za nalaganjem postupanja tijelu javne vlasti radi ostvarivanja takvih prava podnositelja zahtjeva.

Podnositelj zahtjeva kao nezadovoljna stranka podnio je tužbu pred nadležnim upravnim sudom navodeći kako mu ista prava nisu osigurana. Upravni spor je u tijeku.

Primjer 8. – Obradivanje osobnih podataka u svrhu sklapanja pretplatničkog ugovora

Agencija za zaštitu osobnih podataka rješavala je zahtjev za zaštitu prava u kojem je zatraženo utvrđivanje stvarnog potpisnika pretplatničkog ugovora i vjerodostojnosti takvog ugovora.

U ovom predmetu doneseno je rješenje kojim je zahtjev podnositelja odbijen kao neosnovan iz razloga što nije bilo moguće utvrditi da se prikupljeni osobni podaci ne odnose na podnositelja zahtjeva.

Podnositelj zahtjeva kao nezadovoljna stranka podnio je tužbu pred nadležnim upravnim sudom navodeći kako mu ista prava nisu osigurana. Upravni spor je u tijeku.

Primjer 9. – Obrada biometrijskih osobnih podataka

Agencija za zaštitu osobnih podataka rješavala je zahtjev za zaštitu prava vezano uz obradu otiska prsta (*fingerscan*) u svrhu evidencije ulaska u casino.

U ovom predmetu doneseno je rješenje kojim je zahtjev podnositelja ocijenjen kao djelomično osnovan iz razloga što je utvrđeno da podnositelji zahtjeva nisu bili na adekvatan način informirani

o svrsi obrade osobnih podataka posjetitelja casina te je naloženo društvu kao voditelju obrade u čijem je vlasništvu casino da usklade interne akte sa propisima o zaštiti osobnih podataka .
Zahtjev je odbijen u dijelu pribavljanja privole kao zakonite osnove za obradu iz razloga što je za evidenciju ulaska postojala i alternativna evidencija ulaska pomoću tokena.

Nezadovoljna stranka u postupku podnio je tužbu pred nadležnim upravnim sudom navodeći kako mu ista prava nisu osigurana. Upravni spor je u tijeku.

Primjer 10. – Neovlašten uvid i daljnje korištenje osobnih podataka

Agencija za zaštitu osobnih podataka rješavala je zahtjev za zaštitu prava vezano uz obradu osobnih podataka poreznog obveznika od strane poreznog službenika protivno svrsi u koju su podaci prikupljeni od strane poreznog tijela.

U ovom predmetu doneseno je rješenje kojim je zahtjev podnositelja ocijenjen kao osnovan iz razloga što je utvrđeno da je u porezni službenik protivno zakonskim ograničenjima koja proizlaze iz posebnih propisa (Zakon o državnim službenicima, Zakona o Poreznoj upravi, drugim propisima donesenim na temelju zakona i pravilima struke te poštivanja odredbi Etičkog kodeksa državnih službenika i Kodeksa profesionalne etike službenika Ministarstva financija Porezne uprave) neovlašteno vršio uvid u osobne podatke podnositeljice zahtjeva kako porezne obveznice te ih dalje koristio u osobne svrhe.

U tijeku postupka je također utvrđeno kako je porezno tijelo u sklopu svojih obveza kao voditelj obrade osobnih podataka poreznih obveznika poduzeo sve odgovarajuće mjere zaštite kako bi osobni podaci bili odgovarajuće zaštićeni.

Nezadovoljna stranka u postupku podnijela je tužbu pred nadležnim upravnim sudom te je upravni spor u tijeku.

PREPORUKE ZA UNAPREĐENJE ZAŠTITE OSOBNIH PODATAKA

Preporuka 1.

Dostavljanje osobnih podataka/medicinskih nalaza elektroničkom poštom

Agencija je zaprimila upit zdravstvene ustanove vezan za slanje medicinskih nalaza elektroničkim putem, a vezano za postupanja u skladu s novim propisima o zaštiti osobnih podataka, prije svega Opće uredba o zaštiti podataka.

Navedena Opća uredba o zaštiti podataka u članku 4. stavak 1. točka 1. propisuje da su osobni podaci svi podaci koji se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi, a pojedinac čiji se identitet može utvrditi jest osoba koja se može identificirati izravno ili neizravno, osobito uz pomoć identifikatora kao što su ime, identifikacijski broj, podaci o lokaciji, mrežni identifikator ili uz pomoć jednog ili više čimbenika svojstvenih za fizički, fiziološki, genetski, mentalni, ekonomski, kulturni ili socijalni identitet tog pojedinca.

Sukladno odredbama Opće uredbe o zaštiti podataka, osobni podaci moraju biti zakonito, pošteno i transparentno obrađivani s obzirom na ispitanika, prikupljeni u posebne, izričite i zakonite svrhe, primjereni, relevantni i ograničeni na ono što je nužno u odnosu na svrhe u koju se obrađuju, točni i prema potrebi ažurni.

Općom uredbom o zaštiti podataka utvrđeni su uvjeti zakonite obrade osobnih podataka te je opisano šest zakonitih osnova na koje se voditelj obrade može pozvati. Primjena jedne od tih šest osnova mora biti uspostavljena prije aktivnosti obrade u odnosu na posebnu svrhu.

Dakle, vezano za slanje nalaza putem elektroničke pošte, tj. na e-mail adresu pacijenta navodimo kako je voditelj obrade sukladno Općoj uredbi o zaštiti podataka dužan utvrditi postojanje zakonite osnove(dužan prikupiti privolu) ispitanika za obradu osobnih podataka. Ujedno ukazujemo kada/ako je privola ispitanika pravni temelj za obradu osobnih podataka, takva privola ne smije biti uvjetovana (uvažavajući činjenicu kako privola treba predstavljati voljni element ispitanika vezano uz obradu njegovih osobnih podataka) odnosno nužno je da se voditelj obrade u pogledu uvjeta privole pridržava odredbi članka 7. Opće uredbe.

Također ukazujemo na odredbe Opće uredbe o zaštiti podataka kojima je regulirano poduzimanje odgovarajućih mjera zaštite uzimajući u obzir najnovija dostignuća, trošak provedbe te prirodu, opseg, kontekst i svrhe obrade, kao i rizike različitih razina vjerojatnosti i ozbiljnosti za prava i slobode pojedinaca koji proizlaze iz obrade podataka, voditelj obrade, i u vrijeme određivanja sredstava obrade i u vrijeme same obrade, dužan je provoditi odgovarajuće tehničke i organizacijske mjere (primjerice: korisničke lozinke).

Preporuka 2.

Objava osobnih podataka kandidata u natječajnim postupcima

Agencija za zaštitu osobnih podataka došla je do saznanja kako su na internetskoj stranici http://www.zosi.hr/natjecaji/poziv_na_razgovor_natjecaj_od_13092017-66/ objavljen „Poziv na razgovor-natječaj sa imenima i prezimenima kandidata čije su prijave pravovremene i uredne (sadrže sve podatke i isprave) te ispunjavaju uvjete iz natječaja za određena radna mjesta. Dakle, imajući u vidu kako se u konkretnom slučaju radi o objavi imena i prezimena kandidata natječajnog postupka uz pozive za pisana testiranja i intervjue na mrežnoj (web) stranici ova Agencija sukladno svojim zakonskim ovlastima dala je preporuku voditelju obrade da upućivanje poziva kandidatima na testiranje u svrhu provedbe natječaja uputi poštom (primjerice: u zatvorenim kovertama, odnosno, osobno putem elektroničke pošte) ili na način da se raspored testiranja provodi uz poduzimanje odgovarajućih mjera zaštite, primjerice: navodeći prvo slovo prezimena kandidata po abecednom redoslijedu i sl. te smatramo da bi gore navedenim načinom postupanja/disponiranja osobnim podacima kandidata natječaja bila osigurana njihova privatnost i zaštita osobnih podataka u punom opsegu. Zaključno, ova Agencija je istaknula kako je voditelj obrade dužan poduzimati odgovarajuće mjere zaštite i voditi računa da se predmetni osobni podaci mogu koristiti samo u svrhu zbog koje su isti prikupljeni i dalje obrađivani te da se protekom vremena i ostvarivanja svrhe trebaju ukloniti sa mrežne (web) stranice.

Preporuka 3. Korištenje bankovne kartice u svrhu beskontaktnog plaćanja

S obzirom na obraćanje ovoj Agenciji vezano uz pitanje korištenja kartice tekućeg računa koja ima beskontaktnu funkcionalnost, ova Agencija je temeljem članka 33. stavka 1. podstavka 7. Zakona o zaštiti osobnih podataka („Narodne novine“ broj 106/12. – pročišćeni tekst) dala preporuku za unaprjeđenje zaštite osobnih podataka.

U konkretnom slučaju, kako se navodi u očitovanju, banka je u prosincu 2015. godine uvela tehnologiju beskontaktnog plaćanja u poslovanje s individualnim klijentima koji koriste Maestro kartice. Prilikom zamjene Maestro kartica beskontaktnim karticama banka je klijentima omogućila upravljanje beskontaktnom funkcionalnošću na način da je uveden poseban limit za beskontaktna plaćanja, u okviru već postojećeg dnevnog limita za plaćanje Maestro karticama te je klijentima omogućeno upravljanje limitom za beskontaktna plaćanja (mogućnost podnošenja zahtjeva za ukidanjem ili promjenu limita putem e-poslovnice, putem mobilnog bankarstva, telefonskim pozivom, osobno u poslovnicama banke).

Također je navedeno kako je banka klijente obavijestila o namjeri uvođenja beskontaktnog plaćanja prilikom najave izmjena Općih uvjeta poslovanja po transakcijskim računima potrošača koji su bili javno dostupni od 10. srpnja 2015.

Međutim, unatoč navedenoj općenitoj informiranosti ispitanika (klijenata) u ovom slučaju banka je propustila prethodno (prije realizacije predmetne usluge) pribaviti privolu ispitanika (klijenta) vezano upravo uz realizaciju predmetne usluge, pri čemu takva privola mora biti slobodno dana odnosno ne smije biti uvjetovana, a niti unaprijed pretpostavljena. Naime, u slučaju unaprijed pretpostavljene privole klijenata za određene usluge banke, ne možemo govoriti o dobrovoljno i slobodno danoj privoli, odnosno o uvjetima i svojstvima kakva privola mora imati sukladno odredbama Zakona o zaštiti osobnih podataka i Opće uredbe o zaštiti podataka a da bi ista predstavljala pravni temelj za zakonitu obradu osobnih podataka.

Dakle, jasno je kako je odgovorno, savjesno i transparentno upravljanje privolama jedna od temeljnih zadaća voditelja obrade (u ovom slučaju banke). U konkretnom slučaju banka nije postupala pošteno i transparentno u odnosu na klijente, te je koristeći svoju poziciju „jače“ ugovorne strane samoinicijativno nametnula vlastita pravila postupanja, zanemarujući pritom prava klijenata zajamčena Zakonom o zaštiti osobnih podataka i Općom uredbom o zaštiti podataka.

Osim toga, nejasno je kako će klijent ostvariti svoje pravo na povlačenje privole za obradu osobnih podataka ako privolu za uslugu nije niti dao, već je banka pošla od postojanja pretpostavljene privole.

Posebice ističemo kako banka kao voditelj obrade velike količine osobnih podataka velikog broja klijenata mora imati naročito razvijenu svijest o odgovornom upravljanju privolama klijenata, odnosno o nužnosti ispunjavanja svih uvjeta zakonite obrade osobnih podataka a sve kako bi klijenti nesmetano i na transparentan način ostvarili svoja prava na zaštitu osobnih podataka.

Stoga je preporuka ove Agencije da banka prije nuđenja i realizacije određenih usluga prethodno uključi svoje klijente u poslovne procese kako bi u istima klijenti mogli proaktivno sudjelovati i kako bi u svakom trenutku imali sva potrebna saznanja i informacije o okolnostima i uvjetima obrade njihovih osobnih podataka.