REPUBLIKA HRVATSKA
AGENCIJA ZA ZAŠTITU
OSOBNIH PODATAKA

KLASA:
URBROJ:
Zagreb, 06. travnja 2020.

Agencija za zaštitu osobnih podataka na temelju članka 57. stavka 1. i 58. stavka 1. i 2. Uredbe (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka) SLEU L119 (u daljnjem tekstu: Opća uredba), članka 34. Zakona o provedbi Opće uredbe o zaštiti podataka („Narodne novine“, broj: 42/2018) te članka 96. Zakona o općem upravnom postupku („Narodne novine“, broj: 47/09), postupajući po zahtjevu za utvrđivanje povrede prava na zaštitu osobnih podataka xy zastupana po odvjetnicima iz Odvjetničkog društva iz Osijeka, donosi sljedeće

R J E Š E NJ E

1. Zahtjev xy za utvrđivanje povrede prava na zaštitu osobnih podatka je osnovan.

2. Utvrđuje se da je obradom osobnih podataka podnositeljice zahtjeva xy od strane banke na način da su osobni podaci podnositeljice zahtjeva, točnije podaci o stanju na tekućem računu - početni i konačni saldo iskazani na Potvrdi o uplati učinili dostupnima trećoj osobi bez njezinog znanja i pristanka došlo do povrede članka 5.1a) i f) i članka 6. 1. a) Opće uredbe o zaštiti podataka.

3. Nalaže se banci, kao voditelju obrade osobnih podataka poduzimanje odgovarajućih tehničkih i organizacijskih mjera zaštite osobnih podataka u svakodnevnom poslovanju, s ciljem da se zaštite osobni podaci klijenata od slučajnih ili namjernih zlouporaba, neovlaštenih promjena ili dostupa trećim osobama sukladno članku 25. i 32. Opće uredbe o zaštiti podataka.

4. Banci, kao voditelju obrade osobnih podataka, izriče se službena opomena zbog obrade osobnih podataka podnositeljice zahtjeva protivno člancima 5.1.a), 5.1.f) i članku 6.1.a) Opće uredbe o zaštiti podataka.

O b r a z l o ž e nj e

Agencija za zaštitu osobnih podataka zaprimila je zahtjev za utvrđivanje povrede prava na zaštitu osobnih podataka xy zastupana po odvjetnicima iz Odvjetničkog društva iz Osijeka, (dalje u tekstu: podnositeljica zahtjeva) u kojem podnositeljica zahtjeva u bitnome navodi kako je na njezin tekući račun od strane treće osobe uplaćen iznos od 1.870, 00 kuna. Nadalje podnositeljica zahtjeva navodi kako je djelatnik banke (dalje u tekstu: Banka) nakon izvršene uplate trećoj osobi predao potvrdu iz koje je potpuno pregledano stanje na tekućem računu podnositeljice zahtjeva. S tim u vezi, podnositeljica zahtjeva navodi kako su njezini osobni podaci koje je banka prikupila za vođenje kunskog računa, neovlašteno proslijeđeni od strane djelatnika banke trećoj osobi. Podnositeljica zahtjeva navodi kako je za dostavljanje podataka o stanju njezinog salda na računu saznala od treće osobe (kojoj su otkriveni njezini osobni podaci). Podnositeljica navodi da je nakon opisanog događaja 18. prosinca 2018. godine osobno podnijela prigovor banci, poslovnici Šibenik te uz zahtjev za utvrđivanje povrede prava na zaštitu osobnih podataka, kao dokaz svojim navodima dostavlja sljedeće: Punomoć za zastupanje od 21. siječnja 2019. godine; presliku uplate na kunski račun sa naznačenim stanjem na tekućem računu od 18. prosinca 2018. godine; presliku prigovor/reklamacije upućenu banci dana 18. prosinca 2018. godine; presliku odgovora banke na prigovor od 18. prosinca 2018. godine te presliku Zahtjeva za naknadu štete od 31. prosinca 2018. godine i odgovor banke na Zahtjev od 21. siječnja 2019. godine.

Zahtjev je osnovan.

Postupajući po zaprimljenom zahtjevu za utvrđivanje povrede prava na zaštitu osobnih podataka podnositeljice, Agencija za zaštitu osobnih podataka, sukladno svojim ovlastima i zadaćama, zatražila je dopisom KLASA:, URBROJ: od banke očitovanje o postojanju zakonite svrhe i pravne osnove u smislu članka 5. i 6. Opće uredbe o zaštiti podataka za otkrivanje/davanje na korištenje osobnih podataka podnositeljice zahtjeva trećoj osobi, odnosno da pojasne iz kojih razloga i na koji način su prema navodima podnositeljice njeni osobni podaci postali dostupni trećoj osobi. Također, u očitovanju je zatraženo banka pojasni na koji način poduzimaju mjere zaštite osobnih podataka svojih klijenata pritom uzimajući u obzir članak 157. Zakona o kreditnim institucijama („Narodne novine“, broj: 159/13, 19/15, 102/15, 15/18, 70/19).

Agencija za zaštitu osobnih podataka zaprimila je očitovanje od Banke, u kojem navedeno društvo navodi kako je banka 18. prosinca 2018. godine od podnositeljice zahtjeva zaprimila pisani prigovor vezan za predmetnu povredu prava te je bez odgađanja pristupila provjeri okolnosti prigovora. Nadalje, banka navodi kako je treća osoba prilikom provođenja uplate na račun podnositeljice zahtjeva zaprimila potvrdu o uplati, odnosno uplatni listić, na kojem je bilo vidljivo početno i završno stanje na računu na koji je uplata izvršena. Također, navodi kako su podaci na uplatnom listiću uključivali ime i prezime podnositeljice zahtjeva kao vlasnice računa te IBAN račun.

Isto tako u dostavljenom očitovanju predmetno društvo navodi kako je ustanovljeno da je događaj uzrokovala nenamjerna pogreška djelatnika u poslovnici Zagreb. Naime, predmetno društvo navodi, kako je djelatnik pri ručnom unosu podataka potrebnih za transakciju nije adekvatno unio ime nalogodavatelja u sustav, već je kao nalogodavatelj uplate naveden vlasnik računa, a ne treća osoba/uplatitelj što je za posljedicu imalo prikaz stanja računa na uplatnom listiću. S tim u vezi navode kako su ime i prezime vlasnika računa i IBAN bili prethodno poznati trećoj osobi koja je s istima raspolagala prilikom uplate, a što je vidljivo iz obrasca Nalog za uplatu na kunski račun fizičke osobe od strane treće osobe.

Nadalje, predmetno društvo navodi kako je zaključeno da je bila riječ o slučajnoj pogrešci djelatnika do koje je došlo radi previda i odstupanja od propisne interne procedure postupanja banke te je banka poduzela korektivne mjere u vidu dodatnog upozorenja djelatnicima poslovne mreže kako bi se spriječilo ponavljanje daljnjih grešaka ove vrste. Ujedno predmetno društvo ističe, kao je nakon što je ustanovilo da je riječ o povredu osobnih podataka, dana 20. prosinca 2018. godine. obavijestilo Agenciju za zaštitu osobnih podataka putem Izvješća o povredi osobnih podataka unutar 72 sata. Također navode kako je predmetno društvo i podnositeljici zahtjeva odgovorilo u skladu sa rokovima propisanim Općom uredbom o zaštiti podataka.

Nastavno na navedeno, ističemo kako se od 25. svibnja 2018., u svim državama članicama Europske unije, pa tako i u Republici Hrvatskoj, izravno se 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 119.

U članku 4.1. Opće uredbe o zaštiti podataka je navedeno da su osobni podaci 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

Sukladno članku 4.2. Opće uredbe o zaštiti podataka, obrada znači svaki postupak ili skup postupaka koji se obavljaju na osobnim podacima ili na skupovima osobnih podataka, bilo automatiziranim bilo neautomatiziranim sredstvima kao što su prikupljanje, bilježenje, organizacija, strukturiranje, pohrana, prilagodba ili izmjena, pronalaženje, obavljanje uvida, uporaba, otkrivanje prijenosom, širenjem ili stavljanjem na raspolaganje na drugi način, usklađivanje ili kombiniranje, ograničavanje, brisanje ili uništavanje.

Članak 5. Opće uredbe o zaštiti podataka propisuje kako 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 (načelo smanjenja količine podataka), točni i prema potrebi ažurni, 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 (načelo cjelovitosti i povjerljivosti).

Potrebno je referirati se i na članak 6. stavak 1. Opće uredbe o zaštiti podataka koji propisuje kako je obrada osobnih podataka zakonita samo ako i u onoj mjeri u kojoj je ispunjeno najmanje jedno od sljedećeg: 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 pravnih obveza voditelja obrade; 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.

Članak 25. stavak 2. Opće uredbe o zaštiti podataka propisuje kako voditelj obrade provodi odgovarajuće tehničke i organizacijske mjere kojima se osigurava da integriranim načinom budu obrađeni samo osobni podaci koji su nužni za svaku posebnu svrhu obrade. Ta se obveza primjenjuje na količinu prikupljenih osobnih podataka, opseg njihove obrade, razdoblje pohrane i njihovu dostupnost. Točnije, takvim se mjerama osigurava da osobni podaci nisu automatski, bez intervencije pojedinca, dostupni neograničenom broju pojedinca.

Članak 32. stavak 2. Opće uredbe o zaštiti podataka propisuje kako se od strane voditelja i izvršitelja obrade prilikom procjene odgovarajuće razine sigurnosti u obzir posebno uzimaju rizici koje predstavlja obrada, posebno rizici od slučajnog ili nezakonitog uništenja, gubitka, izmjene, neovlaštenog otkrivanja osobnih podataka ili neovlaštenog pristupa osobnim podacima koji su preneseni, pohranjeni ili na drugi način obrađivani.

U ovoj upravnoj stvari nedvojbeno je utvrđeno da društvo obrađuje osobne podatke podnositeljice zahtjeva temeljem ugovornog odnosa. Osobni podaci koji su se obrađivali prilikom ispunjavanja *„Naloga za uplatu na tekući račun fizičke osobe od strane treće osobe“* su: ime i prezime podnositeljice zahtjeva, IBAN račun, te početni i konačni saldo računa.

U postupku je nadalje utvrđeno kako je podnositeljica zahtjeva došla do saznanja da je treća osoba koja je izvršila uplatu na njezin tekući račun putem gore zatraženog Naloga, došla u posjed njezinih podataka, točnije podataka o stanju njezinog tekućeg računa koji je bio iskazan na uplatnom listiću izdanom dana 18. prosinca 2018. godine od strane banke.

U izvješću banke o GDPR incidentu navedeno je kako je treća osoba prilikom uplate na račun klijenta banke, zaprimila potvrdu uplati na kojoj je bilo vidljivo početni i završni saldo predmetnog računa. Vidljivi podaci na uplatnom listiću su ime i prezime vlasnika računa, IBAN računa te početni i završni saldo na tekućem računu. Banka navodi kako su podaci o imenu i prezimenu vlasnika računa kao i njegov IBAN već bili poznati trećoj osobi budući da je ista izvršila uplatu na račun tog klijenta. Također predmetno društvo navodi kako su saznali

za povredu 18. prosinca 2018. godine kada je banka primila pisanu reklamaciju od strane podnositeljice zahtjeva da je treća osoba zaprimila uplatni listić s navedenim početnim i konačnim saldom njegovog računa. Nadalje navode kako je prilikom uplate došlo do slučajne pogreške djelatnika banke jer je kao nalogodavatelja uplate stavljen vlasnik računa, umjesto treća osoba što je posljedično dovelo do prikaza stanja računa na uplatnom listiću.

Sijedom navedenog, **utvrđeno je kako su gore navedenog dana zbog učinjenog grubog propusta zaposlenika banke podaci o stanju tekućeg računa podnositeljice zahtjeva otkriveni trećoj osobi koji je izvršio uplatu na račun podnositeljice zahtjeva**, a što je vidljivo iz ispunjenog „Naloga za uplatu na kunski račun fizičke osobe od strane treće osobe“ koji je isti kao platitelj potpisao. Tom prigodom djelatnik banke je umjesto oznake „treća osoba“ stavio vlasnika računa kao nalogodavatelja uplate te je iz tih razloga došlo do prikaza stanja računa (početni i završni saldo), a što je također vidljivo iz dostavljene potvrde o uplati. Stoga na taj način je došlo do nezakonitog i nepoštenog otkrivanja osobnih podataka, točnije podataka o stanju računa podnositeljice zahtjeva trećoj osobi.

U ovoj upravnoj stvari utvrđeno je kako je opisanim postupanjem **došlo do nezakonite obrade osobnih podataka podnositeljice zahtjeva u navedenu svrhu, a što je za posljedicu imalo neovlašteno omogućavanje uvida u osobne podatke podnositeljice zahtjeva od strane, a sve zbog pogreške djelatnika banke, suprotno članku 5. te članku 6. stavku 1. Opće uredbe o zaštiti podataka.**

Stoga ukazujemo na nužnost unaprjeđenja predmetnog sustava obrade osobnih podataka klijenata banke kako se ne bi događale pogreške/propusti (pristup podacima klijenata od strane treće osobe), a sve u svrhu zaštite osobnih podataka klijenata banke. Ujedno uputno je donošenja pisane procedure/upute za postupanje svih zaposlenika koji obrađuju osobne podatke klijenata banke. S tim u vezi navodimo kako je bitno da voditelj obrade dužan kontinuirano provoditi tehničke i organizacijske mjere zaštite osobnih podataka (primjerice: bilježenje pristupa sustavu, edukacije zaposlenika u obradi osobnih podataka), a sve u svrhu osiguranja provođenja pisanih procedura u obradi osobnih podataka.

Posebice ukazujemo na potrebu kontinuiranog provođenja odgovarajućih tehničkih i organizacijskih mjera zaštite osobnih podataka iz članka 25. stavka 2. i članka 32. stavka 2. Opće uredbe o zaštiti podataka, tj. kontinuirane edukacije osoba zaposlenih u obradi osobnih podataka, prvenstveno u smislu obvezne provjere vođenja točnih, potpunih i ažurnih osobnih podataka, koja utječe na poštenu i zakonitu obradu osobnih podataka klijenata, a naročito u gore opisanim situacijama kada je potrebno provjeriti točnost osobnih podataka koji se upisuju kod provođenja određenih transakcija na računima klijenata kako bi se zaštitili osobni podaci i poštivala i obveza čuvanja bankarske tajne zajamčeno posebnim zakonom.

Slijedom navedenog, u ovoj upravnoj stvari utvrđeno je kako **je banka, kao voditelj obrade osobnih podataka, postupalo protivno odredbama članka 5., 6., 25. i 32. Opće uredbe o zaštiti podataka budući da je u konkretnom slučaju obradom osobnih podataka**

podnositeljice zahtjeva, točnije otkrivanja podataka o stanju/saldu njezinog računa trećoj osobi učinjena gruba povreda prava na zaštitu osobnih podataka. Budući da predmetno društvo prilikom obrade osobnih podataka nije postupalo s pažnjom dobrog gospodarstvenika, odnosno nije naročito savjesno, pouzdano i odgovorno obrađivalo osobne podatke iste što je imalo za posljedicu grubo kršenje privatnosti podnositeljice zahtjeva. Dakle, slijedom navedenih okolnosti, proizlazi kako je banka, kao voditelj obrade osobnih podataka grubo povrijedilo odredbe Opće uredbe o zaštiti podataka iz razloga što je kao voditelj obrade morao znati kakvo takvo postupanje predstavlja kršenje odredbi citirane Uredbe, a time i zadiranje u privatnost podnositeljice zahtjeva.

Budući da je u ovoj upravnoj stvari utvrđeno kako je postupanjem društva došlo do povrede prava na zaštitu osobnih podataka podnositeljice zahtjeva, odnosno do otkrivanja podataka o stanju novčanih sredstava na računu, ova **Agencija je odlučila društvu, kao voditelju obrade izdati službenu opomenu za utvrđeno kršenje prava na zaštitu predmetnih osobnih podataka.**

S obzirom na utvrđenu povredu, Agencija je pristupila izricanju službene opomene prema društvu, smatrajući istu dovoljno svrsishodnom, učinkovitom i dostatnom mjerom kojom će se utjecati na društvo da ubuduće više ne postupa suprotno Općoj uredbi o zaštiti podataka.

Navodimo kako je pri izricanju predmetne korektivne mjere društvu uzeto u obzir da je društvo dana 20. prosinca 2018. godine o učinjenoj povredi osobnih podataka obavijestilo Agenciju za zaštitu osobnih podataka putem Izvješća o povredi osobnih podataka unutar roka propisanog čl. 33. Opće uredbe o zaštiti podataka.

Sukladno iznesenom, odlučeno je kao u Izreci rješenja.

UPUTA O PRAVNOM LIJEKU

Protiv ovog rješenja nije dopuštena žalba, ali se može pokrenuti upravni spor pred Upravnim sudom u roku od 30 dana od dana dostave rješenja.

RAVNATELJ
Anto Rajkovača