**REPUBLIKA HRVATSKA**
**AGENCIJA ZA ZAŠTITU**
**OSOBNIH PODATAKA**
KLASA: UP/I-034-01/23-01/13
URBROJ: 567-12/14-23-01
Zagreb, 15. svibnja 2023.

Agencija za zaštitu osobnih podataka (OIB: 28454963989), na temelju članka 57. stavka 1., članka 58. stavka 1. i 2. točke (i) i članka 83. 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 (dalje u tekstu: Opća uredba o zaštiti podataka) SL EU L119, članka 44., 45. i 46. Zakona o provedbi Opće uredbe o zaštiti podataka ("Narodne novine" br. 42/18) te članka 42. stavka 1. i 2. i članka 96. Zakona o općem upravnom postupku ("Narodne novine" br. 47/09, 110/21) u postupku pokrenutom po službenoj dužnosti protiv voditelja obrade društva Hattrick-PSK d.o.o., Ulica sv. Leopolda Mandića 14, Dugopolje (OIB: 92265244213), radi zaštite osobnih podataka, donosi sljedeće:

**R J E Š E NJ E**

1. Utvrđuje se da je društvo Hattrick-PSK d.o.o., kao voditelj obrade, obrađivalo osobne podatke u vidu preslika bankovnih kartica ispitanika, a za čiju obradu nije dokazana pravna osnova čime je povrijeđen članak 6. stavak 1. Opće uredbe o zaštiti podataka.
2. Utvrđuje se da društvo Hattrick-PSK d.o.o., kao voditelj obrade, nije na adekvatan način obavijestilo ispitanike o obradi osobnih podataka, odnosno o obradi podataka sadržanim na preslikama bankovnih kartica, čime je povrijeđen članak 13. stavak 1. i 2. Opće uredbe o zaštiti podataka.
3. Utvrđuje se da društvo Hattrick-PSK d.o.o., kao voditelj obrade, prilikom kreiranja novog poslovnog procesa za uslugu brze isplate na VISA bankovnu karticu nije implementiralo odgovarajuće tehničke i organizacijske mjere, čime je povrijeđen članak 25. stavak 1. i 2. Opće uredbe o zaštiti podataka.
4. Utvrđuje se da društvo Hattrick-PSK d.o.o., kao voditelj obrade, nije primjenjivalo tehničku mjeru enkripcije na osobne podatke ispitanika pohranjene u bazama podataka voditelja obrade, te nije redovno procjenjivalo učinkovitosti tehničkih i organizacijskih mjera za osiguravanje sigurnosti obrade, a čime je povrijeđen članak 32. stavak 1. toč. a) i d) Opće uredbe o zaštiti podataka.
5. Za kršenja opisana u točkama 1. - 4. izreke ovog rješenja, u skladu s odredbama članka 83. Opće uredbe o zaštiti podataka, izriče se društvu Hattrick-PSK d.o.o., upravna novčana kazna u iznosu od:

**380.000,00 EUR/ 2.863.110,00 kn[1]**

(slovima: tristo osamdeset tisuća eura/dva milijuna osamsto šezdeset tri tisuće sto deset kuna)

[1] Fiksni tečaj konverzije 7,53450 kn

Društvo Hattrick-PSK d.o.o. dužno je platiti izrečenu upravnu novčanu kaznu u korist državnog proračuna u roku od 15 dana od dana pravomoćnosti ovog rješenja u korist računa broj: HR1210010051863000160, model HR64 i poziv na broj odobrenja: 6092-25860-92265244213 s naznakom – "upravne novčane kazne koje izriče AZOP".

6. Ukoliko društvo Hattrick-PSK d.o.o., u roku od 15 dana od pravomoćnosti ovog rješenja ne plati izrečenu upravnu novčanu kaznu, Agencija za zaštitu osobnih podataka će sukladno članku 46. stavku 2. Zakona o provedbi Opće uredbe o zaštiti podataka obavijestiti Područni ured Porezne uprave Ministarstva financija na čijem je području sjedište navedenog društva radi naplate upravne novčane kazne prisilnim putem prema propisima o prisilnoj naplati poreza.

7. Društvo Hattrick-PSK d.o.o. je dužno u roku od 15 dana od izvršene uplate dostaviti dokaz o uplati Agenciji za zaštitu osobnih podataka.

## *Obrazloženje*

## I. UTVRĐENJE POVREDE

Agencija za zaštitu osobnih podataka (dalje u tekstu: Agencija) zaprimila je podnesak građanina odnosan na dopuštenost prikupljanja obostrane preslike bankovne kartice putem elektroničke pošte od strane društva Hattrick-PSK d.o.o. kao voditelja obrade (dalje u tekstu: voditelj obrade).

Nastavno na navedeno, a sukladno danim ovlastima Agencija je pokrenula postupak po službenoj dužnosti zbog visokog rizika za prava i slobode ispitanika (dalje u tekstu: igrači, korisnici usluga) te je u svrhu utvrđenja točnog i potpunog činjeničnog stanja proveo najavljeno nadzorno postupanje kod voditelja obrade, a o čemu je sastavljen Zapisnik KLASA: 042-03/22-01/99, URBROJ: 567-12/09-22-07 od 25. studenog 2022 (dalje u tekstu: Zapisnik).

Tijekom nadzornog postupanja provedenog 23. studenog 2022., u bitnome utvrđeno je sljedeće:

Usluga brze isplate na VISA bankovnu karticu, aktivna je od 20. lipnja 2022. Predmetnom uslugom voditelj obrade omogućio je korisnicima usluge koji imaju otvoren korisnički račun kod voditelja obrade, da nakon što uspješno izvrše uplatu na korisnički račun s VISA bankovnom karticom, na istu VISA bankovnu karticu mogu zatražiti isplatu dobitka, uz potrebnu prethodnu verifikaciju te kartice.

Za verifikaciju VISA bankovne kartice bilo je potrebno skeniranu prednju i stražnju stranicu iste, proslijediti na adresu e-pošte podrska@psk.hr, gdje se unutar nadležne službe voditelja obrade provodila provjera podataka s dostavljene preslike bankovne kartice i podataka korisničkog računa, te je nakon uspješne verifikacije igraču unutar aplikacije omogućeno da odabere isplatu dobitka na tako verificiranu VISA bankovnu karticu.

Voditelj Odjela za praćenje usklađenosti s propisima voditelja obrade naveo je kako su za verifikaciju bankovne kartice nužni podaci u vidu imena i prezimena nositelja kartice, prvi i posljednji niz brojeva kartice uz datum važenja iste.

Proces prikupljanja podataka potrebnih za verifikaciju bankovne kartice provodio se na način da su zaposlenici u Odjelu korisničke podrške predmetnog voditelja obrade, nakon što zaprime poruku igrača sa zahtjevom aktiviranja navedene usluge, igraču odgovarali standardiziranom porukom u kojoj je priložen i slikovni prikaz/primjer bankovne kartice na kojoj je na prednjoj strani crnim pravokutnikom zatamnjen srednji dio niza brojeva bankovne kartice, dok je na stražnjoj strani crnim pravokutnikom zatamnjen CVV broj. Predmetna obavijest sadržava i informacije o trajanju procesa verifikacije kartice, informacije vezane uz isplatu sredstava te informacije za koje bankovne kartice usluga nije dostupna, primjerice Maestro ili Mastercard. U slučaju da igrač dostavi presliku bankovne kartice koja nije prekrivena sukladno danim uputama, igraču zaposlenik šalje poruku da isti dostavi presliku prednje i stražnje strane bankovne kartice sukladno danim mu uputama, te se tek tada preslika bankovne kartice prosljeđuje Odjelu „Fraud/Payment" voditelja obrade. Daljnji proces usporedbe, odnosno provjere podudarnosti podataka o izvršenoj uplati te podataka sadržanih na preslici bankovne kartice (verifikacija bankovne kartice), provodi se u Odjelu „Fraud/Payment", nakon čega zaposlenici navedenog Odjela zaprimljene preslike bankovnih kartica igrača pohranjuju na Share Point koji je smješten u podatkovnom centru voditelja obrade.

Također je utvrđeno da se preslike bankovnih kartica igrača pohranjuju u sustavu pohrane bazi registriranih korisnika usluga/igrača, unutar mape naziva „ " , a neposrednim uvidom u sadržaj mape naziva „ " vidljivo je da ista sadržava 2078 podmapa koje sadrže preslike bankovnih kartica i identifikacijskih isprava.

Tijekom nadzora ovlašteni službenici Agencije zatražili su od voditelja Sektora korisničkih operacija da snimi zaslon poradi evidentiranja svih koraka potrebnih kako bi se ostvario uvid u pohranjene preslike bankovnih kartica i osobnih iskaznica registriranih korisnika usluga/igrača unutra mape .

Voditelj Sektora korisničkih operacija voditelja obrade izjavio je kako je podatkovni centar osiguran odgovarajućim tehničkim mjerama zaštite uključivo elektroničkom bravom i da istomu fizički pristup imaju samo tri ovlaštena zaposlenika voditelja obrade. Nadalje, obzirom da se preslike bankovnih kartica ne spremaju lokalno već samo na gore opisani način, pristup od strane zaposlenika omogućen je udaljenim pristupom podatkovnom centru, a koji je osiguran putem VPN konekcije.

U odnosu na vođenje Evidencija aktivnosti obrade za obradu osobnih podataka, odnosno prikupljanje i pohranu preslika bankovnih kartica igrača, voditelj Odjela za praćenje usklađenosti s propisima, voditelja obrade navodi da za sve obrade osobnih podataka voditelj obrade vodi Evidenciju aktivnosti obrade koja je u formatu Excel tabele te je priložio relevantni izvadak iz iste i naveo kako je opisana obrada preslika bankovnih kartica, odnosno osobnih podataka sadržanih na istima obuhvaćena obradom označenom brojem 744 u priloženom dokumentu koja je temeljena na legitimnom interesu poradi sprječavanja prijevara.

U odnosu na svrhu obrade osobnih podataka i pravnu osnovu za obradu, u svezi poslovnog procesa prikupljanja i pohrane preslika bankovnih kartica igrača, voditelj Odjela za praćenje usklađenosti s propisima voditelja obrade, navodi da voditelj obrade temeljem ugovornog odnosa ili u svrhu sklapanja istog prikuplja od igrača osobne podatke, dok je dio osobnih podataka isti u obvezi prikupiti i temeljem Zakona o sprečavanju pranja novca i financiranja terorizma te Zakona o igrama na sreću i podzakonskih akata donesenih temeljem navedenog Zakona.

Voditelj Odjela pravnih poslova voditelja obrade naveo je da se u konkretnom slučaju radi o ugovornom odnosu sa igračem, te da se mogućnost brze isplate putem VISA bankovne kartice provodi unutar postojećeg ugovornog odnosa sa igračem, jer isti za korištenje te usluge mora biti registrirani korisnik i prikupljanje tih podataka je nužno za provjeru odnosno validaciju korisničkih podataka igrača, a iste pohranjuju poradi mogućnosti dokazivanja zakonitosti obrade.

Dodatno voditelj Odjela pravnih poslova voditelja obrade ukazuje na odredbe članka 24. Pravila igre na sreću klađenjem, koje propisuju koje osobne podatke je voditelj obrade dužan prikupiti kod registracije virtualnog računa igrača, način na koji se ostvaruje pristup korisničkom računu kao i način provedbe uplate i isplate sredstava na virtualni račun igrača kod klađenja na daljinu.

Tijekom nadzornog postupanja voditelj Odjela za praćenje usklađenosti s propisima voditelja obrade priložio je interne akte sačinjene na razini grupacije unutar koje je i predmetni voditelj obrade te naveo kako su iste dužni primjenjivati. Između ostalog priloženi su akti naziva GDPR Politika i Information classification Policy.

U odnosu na konkretan proces obrade bankovnih kartica u svrhu pružanja usluge brze isplate na Visa karticu, predstavnik voditelja obrade dostavio je upute igračima o načinu na koji je potrebno dostaviti preslike bankovnih kartica.

Nadalje, voditelj Odjela za praćenje usklađenosti s propisima voditelja obrade tijekom nadzora je priložio interne akte Pravila privatnosti i Izjavu o mjerama zaštite osobnih podataka, a kojima su igračima pružene informacije o obradi osobnih podataka, a koji akti su i javno dostupni na web stranici odnosno aplikaciji u zasebnom pregledniku voditelja obrade.

Tijekom nadzornog postupanja utvrđeno je kako se u internom aktu Izjava o mjerama zaštite osobnih podataka izričito navodi da voditelj obrade ne pohranjuje brojeve bankovnih kartica i da isti nisu dostupni neovlaštenim osobama.

Voditelj Odjela za praćenje usklađenosti s propisima u voditelju obrade u odnosu na navedeno utvrđenje naveo je kako se dodatne informacije daju zasebno svakom igraču koji zatraži navedenu uslugu od strane zaposlenika Odjela korisničke podrške u direktnoj komunikaciji sa igračem.

Obzirom da tijekom nadzornog postupanja ovlaštenim službenicima nisu bile dostupne sve informacije odnosne na predmetnu obradu, voditelj obrade je bio zapisnikom obvezan dostaviti interne akte, relevantne informacije i dokumentaciju odnosnu na primjenu tehničkih i organizacijskih mjera zaštite osobnih podataka odnosnih na predmetnu obradu osobnih podataka, informacije kako su zaposlenici upoznati sa odredbama odnosnim na zaštitu osobnih podataka, interne akte odnosne na ovlaštenja i upute za rad zaposlenika, kao i informacije u odnosu na način provođenja nadzornog postupanja, a koje informacije je Agencija zaprimila uz očitovanje predmetnog voditelja obrade od 7. prosinca 2022. (dalje u tekstu: prvo očitovanje)

U prvom očitovanju voditelj obrade u bitnom navodi kako su zaposlenici koji obrađuju osobne podatke upoznati s relevantnim internim politikama u kojima je definiran prihvatljiv način korištenja informacija, uređaja i mreža koje koriste prilikom obavljanja redovnih radnih aktivnosti, a koji interni akti su priloženi u nadzornom postupanju. Od internih akata voditelj

obrade izdvaja akt naziva GDPR Politika za koji navodi da propisuje specifične tehničke i organizacijske mjere te načine primjene načela zaštite osobnih podataka. U odnosu na ovlaštenja za rad zaposlenika na obradi osobnih podataka navodi se kako su ista regulirana Odlukom o organizaciji, sistematizaciji i opisu radnih mjesta društva, a provođenje takvih mjera osigurano je informatičko tehničkom zaštitom koje osiguravaju pristup samo ovlaštenim osobama.

Nadalje, u prvom očitovanju u odnosu na organizacijske mjere voditelj obrade upućuje na interne akte GDPR Politika, FEG Information resource acceptable use Policy, Information security risk Management Policy, Patch and vulnerability Management Policy, Information classification Policy.

U odnosu na utvrđenje iz Zapisnika o pohranjenim preslikama bankovnih kartica na kojima su uz ostale podatke vidljivi i cjeloviti broj bankovne kartice, datum važenja bankovne kartice i CVV broj, voditelj obrade navodi kako su u procesu kreiranja i implementiranja kontrolnih procesa koji će osigurati kontrolu operativnog izvođenja relevantnih radnji na redovnoj bazi, a sve u svrhu otklanjanja nepravilnosti.

Dodatno voditelj obrade u prvom očitovanju navodi kako su zaposlenici prošli edukaciju te su uz prvo očitovanje priložene potvrde o obuci te izjave o povjerljivosti potpisane od strane zaposlenika koji su bili uključeni u proces obrade osobnih podataka. Ujedno ukazuje i na činjenicu kako je voditelj obrade ugovorom o radu obvezao zaposlenike na obvezu čuvanja tajnosti podataka prikupljenih prilikom obavljanja radnih zadaka, uz predviđene ugovorne kazne u slučaju kršenja te obveze.

Prvom očitovanju voditelj obrade priložio je i interne upute za zaposlenike voditelja obrade naziva „Proces isplate na VISA bankovne kartice". Uvidom u sadržaj dostavljenog dokumenta utvrđeno je kako isti sadrži upute zaposlenicima da od ispitanika zatraže dostavu djelomično prekrivene preslike bankovne kartice, uputu da obrišu zaprimljenu presliku bankovne kartice u slučaju da ista nije prekrivena sukladno danim uputama te upute na koji način verificirati dostavljene podatke te iste unesu u informacijski sustav (IMS).

Nadalje, Zapisnikom su zatražene i dodatne informacije o svrsi i pravnom temelju predmetne obrade, o opsegu osobnih podataka koji je nužan za obradu te evidenciju aktivnosti obrade odnosnu na predmetnu obradu.

U odnosu na pravnu osnovu za predmetnu obradu (prikupljanje i pohrana preslika bankovnih kartica) voditelj obrade je naveo kako se radi o obradi koja je nužna za izvršavanje ugovora, odnosno korištenje specifične usluge – brze isplate na VISA bankovnu karticu te je izričito zanijekao legitimni interes kao pravnu osnovu.

Voditelj obrade u prvom očitovanju navodi kako se nužni set podataka potrebnih za predmetnu obradu sastoji od prva i zadnja četiri broja kartice, imena i prezimena nositelja kartice i datum važenja iste, dok kao svrhu obrade preslika bankovnih kartica navodi verifikaciju podataka sadržanih na bankovnoj kartici nužnih za aktiviranje opcije VISA brze isplate, odnosno potvrda identiteta fizičke osobe koja koristi korisnički račun, a poradi poštivanja odredbi članak 24. Pravila igre na sreću klađenje.

Također, voditelj obrade u prvom očitovanju ističe kako ima zakonsku obvezu utvrditi identitet osobe koja koristi korisnički račun, te kako je sukladno Zakonu o sprečavanju pranja novca i financiranja terorizma dužan prikupljati podatke o izvorima sredstava.

Nadalje, u prvom očitovanju se navodi kako je obrada osobnih podataka u vidu preslika bankovnih kartica u Evidenciji aktivnosti obrade označena br. 1017 pod obradom naziva Communication with customer (hrv. Komunikacija s kupcem).

Zaključno Zapisnikom je zatražena i dostava informacija o načinu na koji su ispitanici obaviješteni o obradi osobnih podataka, kao i sadržaj komunikacije ostvarene s igračem putem e-pošte podrska@psk.hr pri prikupljanju podataka.

Voditelj obrade u prvom očitovanju navodi kako odredbe Politike privatnosti i Izjava o mjerama zaštite kojima je ispitanicima dana obavijest kako se podaci o bankovnim karticama ne prikupljaju, odnose na uplatu sredstava. Dok je o predmetnoj obradi u svrhu isplate sredstava ispitanik obaviješten kada zatraži uslugu brze isplate na VISA karticu putem standardizirane obavijesti.

Agencija je dopisom KLASA:042-03/22-01/99, URBROJ:567-12/09-22-09 od 08. prosinca 2022., a u skladu sa svojim ovlastima, između ostalog, zatražila od voditelja obrade dostavu kopije sadržaja datoteke mape naziva „ ?“, internih akata koji sadrže konkretne odredbe kojima je propisana odgovornost nadgledanja (i sam postupak) nad postupanjem zaposlenika voditelja obrade u odnosu na konkretnu obradu i očitovanje zašto isto nije provođeno, te informacije iz kojih propisa proizlazi zakonska obveza prikupljanja i pohrane preslika bankovnih kartica za voditelja obrade.

U odnosu na zatraženo, Agencija je dana 14. prosinca 2022. zaprimila od voditelja obrade kopiju sadržaja datoteke mape naziva „ “, čiji je sadržaj analiziran, a o čemu je sastavljena službena bilješka KLASA: 042-03/22-01/99, URBROJ: 567-12/13-23-12 od datuma 27. veljače 2023.

Nadalje, Agencija je 23. prosinca 2022. zaprimila od voditelja obrade očitovanje (u daljnjem tekstu: treće očitovanje) odnosno na konkretne odredbe kojima je propisana odgovornost nadgledanja (i sam postupak) nad postupanjem zaposlenika voditelja obrade u odnosu na konkretnu obradu vezanu za uslugu VISA brze isplate. Voditelj obrade očitovao se kako je postupak nadgledanja nad postupanjem zaposlenika voditelja obrade u odnosu na konkretnu obvezu proizlazi iz radno-pravne obveze onih koji predmetnu obradu provode, a odgovornost nadgledanja obveza je njihovih neposrednih rukovoditelja. Nadalje se pojašnjava kako postupak nadgledanja ispunjenja radnih obveza nije izričito propisan internim aktima voditelja obrade, no sastoji se od tjednih kolegija, nenajavljenih kontrola procesa rada te informacija o provođenju radnih obveza, a o čemu se ne sastavlja zapisnik ukoliko nije došlo do povrede koju je nužno dokumentirati.

U odnosu na navedeno, voditelj obrade također navodi kako je rukovoditelj Sektora korisničkih operacija redovito ustanovljavao kako je postupanje zaposlenika u vezi predmetne obrade bilo usklađeno s propisnima.

Nadalje voditelj obrade ističe kako nije imao utjecaja na činjenicu da pojedini igrači nisu postupili sukladno danim uputama, odnosno dostavljali presliku bankovne kartice sukladno danim uputama, te da voditelj obrade nije zaprimio nepropisno zatamnjene bankovne kartice

uslijed greške svojih zaposlenika. Iz naprijed navedenog razloga smatraju da odgovornost ne može biti na voditelju obrade. Svoju odgovornost smatraju isključivo u osiguranju najvišeg stupnja zaštite pohrane bankovnih kartica.

U odnosu na konkretne zakonske obveze iz koje proizlazi nužnost prikupljanja i pohrane preslika bankovnih kartica voditelj obrade navodi odredbe članka 15. stavak 1. toč. 4., članka 16. stavak1. toč. 4., članka 20. stavak 8., članka 20. stavak 1. toč. 2.,10. i 11., članka 21. Zakona o sprječavanju pranja novca i financiranju terorizma („Narodne novine", br. 108/17, 39/19).

Zaključno, voditelj obrade u trećem očitovanju navodi da je proveo analizu cjelokupnog procesa usluge VISA brze isplate, nakon čega su izvršena dodatna ulaganja u procese plaćanja na način da je sustav unaprijeđen te se u pogledu platnih operacija VISA karticom primjenjuje 3D Secure - protokol za online transakcije bankovnim i debitnim karticama, a što podrazumijeva da se od igrača više ne traži dostava preslike bankovnih kartica. Nadalje, voditelj obrade naveo je kao je obrisao prikupljene preslike bankovnih kartica.

Agencija ističe da se od 25. svibnja 2018. godine u svim državama članicama Europske unije, pa tako i u Republici Hrvatskoj, izravno i obvezujuće 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 osobnih podataka (SL EU L119)).

Sukladno članku 4. stavku 1. točki 1. Opće uredbe o zaštiti podataka, osobni podaci su 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 članku 4. stavku 1. točki 2. Opće uredbe o zaštiti podatka, 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.

Člankom 6. stavkom 1. Opće uredbe o zaštiti podataka 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 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.

Sukladno članku 6. stavku 3. Opće uredbe o zaštiti podataka ako je pravni temelj za obradu osobnih podataka pravna obveza voditelja obrade ili izvršavanje zadaće od javnog interesa/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.

Člankom 13. stavak 1. Opće uredbe o zaštiti podataka propisana je obveza za voditelja obrade da u trenutku prikupljanja osobnih podataka ispitaniku pruži sve sljedeće informacije:
(a) identitet i kontaktne podatke voditelja obrade i, ako je primjenjivo, predstavnika voditelja obrade;
(b) kontaktne podatke službenika za zaštitu podataka, ako je primjenjivo;
(c) svrhe obrade radi kojih se upotrebljavaju osobni podaci kao i pravnu osnovu za obradu;
(d) ako se obrada temelji na članku 6. stavku 1. točki (f), legitimne interese voditelja obrade ili treće strane;
(e) primatelje ili kategorije primatelja osobnih podataka, ako ih ima; i
(f) ako je primjenjivo, činjenicu da voditelja obrade namjerava osobne podatke prenijeti trećoj zemlji ili međunarodnoj organizaciji te postojanje ili nepostojanje odluke Komisije o primjerenosti, ili u slučaju prijenosâ iz članaka 46. ili 47. ili članka 49. stavka 1. drugog podstavka upućivanje na prikladne ili odgovarajuće zaštitne mjere i načine pribavljanja njihove kopije ili mjesta na kojem su stavljene na raspolaganje.

Stavkom 2. istog članka propisano je kako voditelj obrade treba pružiti ispitaniku i dodatne informacije potrebne kako bi se osigurala poštena i transparentna obrada:
(a) razdoblje u kojem će osobni podaci biti pohranjeni ili, ako to nije moguće, kriterije kojima se utvrdilo to razdoblje;
(b) postojanje prava da se od voditelja obrade zatraži pristup osobnim podacima i ispravak ili brisanje osobnih podataka ili ograničavanje obrade koji se odnose na ispitanika ili prava na ulaganje prigovora na obradu takvih te prava na prenosivost podataka;
(c) ako se obrada temelji na članku 6. stavku 1. točki (a) ili članku 9. stavku 2. točki (a), postojanje prava da se u bilo kojem trenutku povuče privolu, a da to ne utječe na zakonitost obrade koja se temeljila na privoli prije nego što je ona povučena;
(d) pravo na podnošenje prigovora nadzornom tijelu;
(e) informaciju o tome je li pružanje osobnih podataka zakonska ili ugovorna obveza ili uvjet nužan za sklapanje ugovora te ima li ispitanik obvezu pružanja osobnih podataka i koje su moguće posljedice ako se takvi podaci ne pruže;
(f) postojanje automatiziranog donošenja odluka, što uključuje izradu profila iz članka 22. stavaka 1. i 4. te, barem u tim slučajevima, smislene informacije o tome o kojoj je logici riječ, kao i važnost i predviđene posljedice takve obrade za ispitanika.

Odredbe stavka 4. istog članaka oslobađaju voditelja obrade od gore opisanih obveza ako i u onoj mjeri u kojoj ispitanik već raspolaže informacijama.

Sukladno članku 24. stavku 1. i 2. Opće uredbe o zaštiti podataka, uzimajući u obzir prirodu, opseg, kontekst i svrhe obrade, kao i rizike različitih razina vjerojatnosti i ozbiljnosti za prava i slobode pojedinaca, voditelj obrade provodi odgovarajuće tehničke i organizacijske mjere kako bi osigurao i mogao dokazati da se obrada provodi u skladu s ovom Uredbom. Te se mjere prema potrebi preispituju i ažuriraju.

Ako su razmjerne u odnosu na aktivnosti obrade, mjere iz stavka 1. uključuju provedbu odgovarajućih politika zaštite podataka od strane voditelja obrade.

Člankom 25. Opće uredbe o zaštiti podataka propisano je kako voditelj obrade 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, i u vrijeme određivanja sredstava obrade i u vrijeme same obrade, provodi odgovarajuće tehničke i organizacijske mjere, poput pseudonimizacije, za omogućavanje učinkovite primjene načela zaštite podataka, kao što je smanjenje količine podataka, te uključenje zaštitnih mjera u obradu kako bi se ispunili zahtjevi iz ove Uredbe i zaštitila prava ispitanika.

Nadalje, stavak 2. istog članka propisuje da 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 1. Opće uredbe o zaštiti podataka propisuje da 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, uključujući prema potrebi: (a) pseudonimizaciju i enkripciju osobnih podataka i (d) proces za redovno testiranje, ocjenjivanje i procjenjivanje učinkovitosti tehničkih i organizacijskih mjera za osiguravanje sigurnosti obrade.

Člankom 15. Zakona o sprječavanju pranja novca i financiranja terorizma propisano je:
„(1) Dubinska analiza stranke obuhvaća sljedeće mjere, ako nije drukčije propisano ovim Zakonom:
....
4. stalno praćenje poslovnoga odnosa, uključujući i kontrolu transakcija koje stranka obavlja tijekom poslovnoga odnosa kako bi se osiguralo da su transakcije koje se obavljaju u skladu sa saznanjima obveznika o stranci, poslovnome profilu, profilu rizika, uključujući prema potrebi i podatke o izvoru sredstava, pri čemu dokumentacija i podatci kojima obveznik raspolaže moraju biti ažurni.“

Člankom 16. Zakona o sprječavanju pranja novca i financiranja terorizma propisano je:
(1) Obveznik iz članka 9. ovoga Zakona je dužan, pod uvjetima određenima ovim Zakonom i na temelju njega donesenim podzakonskim aktima, obaviti dubinsku analizu stranke u sljedećim slučajevima:
.....
4. u pružanju usluga igara na sreću, prilikom stavljanja uloga i preuzimanja dobitaka, uključujući kupnju ili zamjenu žetona u kunskoj vrijednosti od 15.000,00 kuna i većoj bez obzira na to je li riječ o jednokratnoj transakciji ili o više transakcija koje su međusobno očigledno povezane i koje ukupno dosežu vrijednost od 15.000,00 kuna i veću

Člankom 20. Zakona o sprječavanju pranja novca i financiranja terorizma propisano je:
„(1) Obveznik iz članka 9. ovoga Zakona pri obavljanju dubinske analize stranke prikuplja sljedeće podatke:
.....
2. za fizičku osobu kojoj je namijenjena transakcija: ime i prezime, prebivalište te podatak o identifikacijskome broju fizičke osobe ako mu je taj podatak dostupan

...
10. datum i vrijeme provedbe transakcije, iznos i valutu u kojoj se obavlja transakcija, način provedbe transakcije te, kada obveznik na temelju procjene rizika provedene sukladno odredbama ovoga Zakona i na temelju njega donesenih podzakonskih akata utvrdi visoki rizik od pranja novca ili financiranja terorizma, svrhu (namjenu) transakcije
11. o izvoru sredstava koja jesu ili će biti predmet poslovnoga odnosa
...
(8) Obveznik iz članka 9. stavka 2. točke 16. ovoga Zakona u okviru dubinske analize stranke prilikom provođenja transakcije iz članka 16. stavka 1. točke 4. ovoga Zakona prikuplja podatke iz stavka 1. točaka 1., 2., 3. b), 5., 6. i 10. ovoga članka."

Člankom 21. Zakona o sprječavanju pranja novca i financiranja terorizma propisano je:
„(1) Za stranku koja je fizička osoba i njezina zakonskoga zastupnika te stranku koja je obrtnik ili osoba koja se bavi drugom samostalnom djelatnošću obveznik utvrđuje i provjerava njezin identitet prikupljanjem podataka iz članka 20. stavka 1. točke 1. ovoga Zakona uvidom u službeni osobni dokument stranke u njezinoj nazočnosti.
(2) Ako uvidom u službeni osobni dokument nije moguće prikupiti sve propisane podatke, nedostajući podatci prikupljaju se iz drugih važećih javnih isprava koje podnese stranka.
(3) Kada obveznik iz objektivnih razloga ne uspije prikupiti podatak u skladu sa stavcima 1. i 2. ovoga članka, takav podatak može prikupiti neposredno od stranke, te je dužan poduzeti razumne mjere za provjeru toga podatka.
(4) Ako je stranka obrtnik ili osoba koja se bavi drugom samostalnom djelatnošću, obveznik prikuplja podatke iz članka 20. stavka 1. točke 3. ovoga Zakona uvidom u izvornik ili ovjerenu presliku dokumentacije iz obrtnoga ili drugoga javnog registra koja dokumentacija ne smije biti starija od tri mjeseca, odnosno neposrednim uvidom u obrtni ili drugi javni registar. Na izvodu iz registra u koji je izvršen neposredni uvid obveznik u obliku zabilješke upisuje datum i vrijeme te ime i prezime osobe koja je izvršila uvid."

Člankom 79. Zakona o sprječavanju pranja novca i financiranja terorizma propisano je:
„(1) Obveznik iz članka 9. ovoga Zakona dužan je podatke, informacije i dokumentaciju prikupljenu primjenom ovoga Zakona i na temelju njega donesenih podzakonskih akata i Uredbe (EU) 2015/847 čuvati deset godina nakon prestanka poslovnoga odnosa, obavljanja transakcije iz članka 16. stavka 1. točaka 2., 3. i 4. ovoga Zakona, prikupljanja podataka iz članka 16. stavka 2. ovoga Zakona ili pristupa sefu iz članka 27. ovoga Zakona.
(2) Dokumentacija iz stavka 1. ovoga članka mora sadržavati:
1. dokumentaciju na temelju koje je utvrđen identitet stranke (preslika službenoga osobnog dokumenta, preslika izvoda iz sudskoga ili drugoga registra i dr.)
2. podatke i dokumentaciju o poduzetim mjerama utvrđivanja stvarnoga vlasnika stranke
3. dokumentaciju o poslovnim odnosima i računima stranke
4. dokumentaciju o poslovnoj korespondenciji obveznika sa strankom
5. zapise i evidenciju potrebnu za identifikaciju i praćenje nacionalnih i prekograničnih transakcija
6. dokumentaciju koja se odnosi na utvrđivanje pozadine i svrhe složenih i neobičnih transakcija te rezultate analize tih transakcija
7. drugu pripadajuću dokumentaciju dobivenu prilikom provođenja mjera dubinske analize stranke ili provođenja pojedinačnih transakcija i
8. ako postoje, informacije dobivene sredstvima elektroničke identifikacije, relevantnim uslugama povjerenja kako je propisano Uredbom (EU) 910/2014 te bilo kojim drugim sigurnim, daljinskim ili elektroničkim postupkom identifikacije koji su regulirala, priznala, odobrila ili prihvatila relevantna nadležna tijela.

(3) Obveznik je dužan pet godina čuvati podatke i odgovarajuću dokumentaciju o ovlaštenoj osobi i zamjeniku ovlaštene osobe, procjeni rizika stranke, stručnome osposobljavanju i izobrazbi zaposlenika i provođenju unutarnje revizije.
(4) Obveznik je dužan nakon isteka rokova utvrđenih u stavcima 1. i 3. ovoga članka osobne podatke o stranci brisati, a dokumentaciju iz stavka 2. ovoga članka uništiti u skladu sa zakonom koji uređuje zaštitu osobnih podataka."

U ovoj upravnoj stvari utvrđeno je kako je voditelj obrade od lipnja do prosinca 2022. igračima pružao dodatnu uslugu isplate dobitka, osvojenog temeljem ugovora o sudjelovanju u igri na sreću – klađenjem, na VISA bankovnu karticu, a pored već postojećih mogućnosti isplate u vidu pružanja isplate novčanih sredstava sa korisničkog računa na bankovni račun, Skrill-a, Aircash-a i putem poslovnice.

Utvrđeno je kako obrada u vidu prikupljanja preslika bankovnih kartica nije nužna za ispunjenje ugovora o sudjelovanju u igri između ispitanika (igrača) i voditelja obrade (kao priređivača igre na sreću klađenjem) s obzirom da se radi o samo jednoj od opcija isplate dobitka sa korisničkog računa, a koji je ispitanik (igrač) stekao temeljem ugovora o sudjelovanju u igri.

Utvrđeno je i kako obrada u vidu prikupljanja preslika bankovnih kartica nije nužna radi poštivanja zakonskih obveza koje proizlaze iz Zakona o sprječavanju pranja novca, s obzirom da se dubinska analiza ispitanika može provesti i bez prikupljanja obostranih preslika bankovnih kartica.

U odnosu na informacije koje su ispitanicima bile pružene vezane za konkretnu obradu preslika bankovnih kartica utvrđeno je kako je u Izjavi o mjerama zaštite osobnih podataka, koja čini dio Politike privatnosti, izričito bilo navedeno kako voditelj obrade ne pohranjuje brojeve bankovnih kartica i da brojevi nisu dostupni neovlaštenim osobama. Predmetni akti bili su dostupni ispitanicima na internet stranicama voditelja obrade.

Također, utvrđeno je da standardizirana obavijest koji su igrači zaprimili prilikom traženja isplate na VISA bankovnu karticu sadržava slikovnu uputu na koji način dostaviti presliku, informacije o trajanju procesa verifikacije kartice, informacije o ograničenjima prilikom isplate sredstava te informacije za koje bankovne kartice usluga nije dostupna.

Utvrđeno da se prikupljanje podataka (obostrane preslike bankovnih kartica) obavljalo putem sredstava elektroničke pošte podrska@psk.hr, na način da su igrači nakon što su zatražili opciju isplate na VISA bankovnu karticu dobili standardiziranu uputu (prileži spisu) koja je sadržavala slikovni prikaz bankovne kartice na kojoj je na prednjoj strani crnim pravokutnikom zatamnjen srednji dio niza brojeva bankovne kartice, dok je na stražnjoj strani crnim pravokutnikom zatamnjeno polje koje sadrži kontrolni broj.

Utvrđeno je kako je voditelj obrade dao uputu naziva „Proces isplate na VISA bankovne kartice" (prileže spisu). Sukladno danim uputama preslike bankovnih kartica zaposlenici odjela korisničke podrške prosljeđivali su zaposlenicima odjela „Fraud/Payment" zbog daljnjeg procesa verifikacije bankovne kartice, manualnom usporedbom podataka o izvršenoj uplati te podataka sadržanih na preslici bankovne kartice.

Također, čitanjem Odluke o organizaciji, sistematizaciji i opisu radnih mjesta društva od 10. prosinca 2021., utvrđeno je kako je člankom 5. definirano da je Rukovoditelj Sektora

korisničkih operacija zadužen za svakodnevno nadgledanje aktivnosti u odjelu korisničke podrške kako bi se umanjio broj ljudskih grešaka (prileži spisu).

Nadalje, čitanjem internog akta voditelja obrade naziva Information classification Policy (hrv. Politika klasifikacije podataka) utvrđeno je kako su financijski podaci i osobni podaci korisnika usluga kategorizirani kao „Confidential" (hrv. povjerljivi) te je kao tehnička mjera propisana enkripcija podataka koja se treba primjenjivati pri pohranjivanju povjerljivih elektroničkih dokumenata, kao i prilikom slanja povjerljivih podataka putem elektroničke pošte. (Information classification Policy str. 9. i 11., prileži spisu).

Analizom snimki zaslona (prilog 3. Zapisnika prileži spisu) kojima su evidentirani svi koraci potrebni kako bi se ostvario uvid u pohranjene preslike bankovnih kartica i osobnih iskaznica registriranih korisnika usluga/igrača unutra mape , vidljivo je kako je voditelj Sektora korisničkih operacija, pristupio bazi registriranih korisnika usluga/igrača, na način da je pristupio mrežnom disku naziva , na kojem je između ostalih bila dostupna mapa a unutar koje se nalazi mapa .

Nadalje, klikom na ikonu mape prikazan je sadržaj iste u vidu podmapa odnosnih na pojedinačne igrače. Otvaranjem nasumično odabranih podmapa koje se odnose na pojedine igrače dobivaju se na uvid preslike osobnih dokumenata i bankovnih kartica u izvornom obliku.

Analizom prethodno opisanih koraka utvrđeno je kako sustav nije zatražio unos lozinke za pristup mapi , odnosno da mapa nije bila zaštićena od neovlaštenog pristupa lozinkom.

Nadalje, otvaranjem nasumično odabranih podmapa vidljivo je kako su unutar istih sadržane datoteke u izvornom obliku na koje nije bio primijenjen algoritam za enkripciju tj. iste nisu pohranjene u kriptiranom formatu.

Nadalje, analizom ovlaštenih službenika Agencije sadržaja naknadno dostavljenih datoteka unutar mape naziva , ", utvrđeno je kako su pohranjene preslike identifikacijskih dokumenata za 27 igrača, kao i preslike bankovnih kartica (VISA, MAESTRO, MASTERCARD) za 2078 igrača, od čega 52 bankovne kartice MAESTRO i MASTERCARD koje uopće nisu podržane uslugom brze VISA isplate, a na 665 pohranjenih preslika bankovnih kartica je vidljiv i verifikacijski broj bankovne kartice, koji je jedinstveni 3 ili 4-znamenkasti broj otisnut na kartici uz broj računa koji služi kao dokaz o fizičkom posjedovanju kartice u trenutku online kupnje kojim se smanjuje mogućnost prijevare (Službena bilješka KLASA: 042-03/22-01/99, URBROJ:567-12/13-23-12 od dana 27. veljače 2023. prileži spisu).

U ovom upravnom postupku voditelj obrade pokušao je dokazati kako je obrada u vidu prikupljanja i pohrane preslika bankovnih kartica nužna za izvršavanje ugovora u vidu usluge brze isplate na VISA bankovnu karticu, a pored toga i zakonska obveza koja proizlazi iz obveze provođenja dubinske analize sukladno Zakonu o sprječavanju pranja novca i financiranja terorizma.

U odnosu na konkretne odredbe ugovora koje ukazuju na nužnost predmetne obrade voditelj obrade se poziva na članak 24. Pravila igre na sreću klađenja. Sukladno navedenoj odredbi voditelj obrade zadržava pravo provjere podataka imena i prezimena na bankovnoj kartici igrača, kako bi osigurao poštivanje pravila igre da ime i prezime na virtualnom računu igrača mora biti identično imenu i prezimenu na bankovnoj kartici igrača koje se koriste u svrhu novčanih transakcija ukoliko se uplate/isplate vrše putem bankovnih kartica.

U odnosu na pravnu osnovu u vidu pravne obveze pozivaju se na odredbe članaka 15. stavak 1. toč. 4., članka 16. stavak1. toč. 4., članak 20. stavak 8., članak 20. stavak 1. toč. 2.,10. i 11., članka 21. Zakona o sprječavanju pranja novca i financiranju terorizma.

Sukladno uvodnim odredbama Pravila igre na sreću klađenjem propisano je kako su Pravila igre na sreću klađenjem isključivi zakonski i pravni temelj za zaključivanje ugovora o sudjelovanju u igri, a koji se zaključuje između priređivača (voditelja obrade) i igrača (ispitanika) na osnovi prihvata odredbi Pravila igre na sreću klađenjem te se isti smatra sklopljenim u trenutku zaključenja oklade, odnosno uplatom listića.
Nadalje, uslugu VISA brze isplate moguće je ostvariti samo na bankovnu karticu s koje je izvršena uplata za klađenje od strane igrača s postojećim korisničkim računom otvorenim kod voditelja obrade, slijedom čega se može zaključiti kako se radi samo o jednoj od opcija isplate dobitka osvojenog temeljem ugovora o sudjelovanju u igri.

Slijedom navedenog, Agencija ne može prihvatiti obrazloženje voditelja obrade kako je prikupljanje i pohrana preslika bankovnih kartica nužno za izvršenje ugovora u vidu pružanja usluge VISA brze isplate sredstava s korisničkog računa ispitanika, kao zasebnog ugovora u odnosu na ugovor koji se zaključuje između priređivača igre na sreću (voditelja obrade) i igrača (ispitanika) na osnovi prihvata Pravila igre na sreću klađenjem.

Nadalje, poredbeno ne mogu se prihvatiti ni navodi kako je isto nužno za izvršenje u vidu pružanja usluge VISA brze isplate, a uzimajući u obzir dostupnost online usluga za provedbu novčanih transakcija.

Nije sporno da voditelj obrade kako bi osigurao poštivanje pravila igre klađenja mora provjeriti je li ime i prezime na virtualnom računu igrača identično imenu i prezimenu na bankovnoj kartici igrača koje se koriste u svrhu novčanih transakcija ukoliko se uplate/isplate vrše putem bankovnih kartica.

Nije sporno ni da dubinska analiza prema potrebi može uključivati i podatke o izvoru sredstava te datum i vrijeme provedbe transakcije, iznos i valutu u kojoj se obavlja transakcija, način provedbe transakcije te, kada obveznik na temelju procjene rizika utvrdi visoki rizik od pranja novca ili financiranja terorizma, svrhu (namjenu) transakcije, a sukladno relevantnim odredbama na koje je ukazao voditelj obrade. No, analizom predmetnih članaka Zakona o sprječavanju pranja novca i financiranju terorizma Agencija nije prenašala elemenata koji bi ukazivali na postojanje pravne obveze u vidu prikupljanja i pohrane preslika bankovnih kartica.

Zakon o sprječavanju pranja novca i financiranja terorizma u članku 79. propisuje obvezu čuvanja preslika službenoga osobnog dokumenta na temelju kojeg je utvrđen identitet stranke 10 godina, no istim člankom nije propisana obveza čuvanja preslike bankovne kartice.

Predmetna obrada je uključivala prikupljanje i pohranu prekomjernog opsega podataka u vidu preslika bankovnih kartica, a na kojima je sadržan širi opseg osobnih podataka od onih koji su nužni za izvršenje ugovora, odnosno poštivanje pravnih obveza, slijedom čega je utvrđeno kršenje članka 6. Opće uredbe o zaštiti podataka.

Tom utvrđenju u prilog govore i navodi voditelja obrade kako je obrisao sve pohranjene preslike bankovnih kartica.

Sukladno uvodnoj izjavi (60) Opće uredbe o zaštiti podataka, a koja je odnosna na članak 13. Opće uredbe o zaštiti podataka voditelj obrade ima obvezu informirati ispitanika o postupku obrade i njegovim svrhama te bi trebao ispitaniku pružiti sve dodatne informacije neophodne za osiguravanje poštene i transparentne obrade.

U konkretnom slučaju voditelj obrade tvrdio je kako su ispitanicima informacije o obradi osobnih podataka pružene kroz akte Politika privatnosti i Izjava o mjerama zaštite osobnih podataka te kroz standardiziranu obavijest koju bi zaprimili prilikom traženja isplate na VISA bankovnu karticu.

Uvidom u relevantnu dokumentaciju voditelja obrade utvrđeno je kako ista ne sadrži informacije o pravnoj osnovi, svrsi, razdoblju pohrane preslika bankovnih kartica, kao ni informacije o tome je li pružanje preslika bankovnih kartica zakonska ili ugovorna obveza ili uvjet nužan za sklapanje ugovora, a slijedom čega je utvrđeno kršenje članka 13. stavka 1. i 2. Opće uredbe o zaštiti podataka.

Sukladno odredbama članka 25. Opće uredbe o zaštiti podataka voditelj obrade je obvezan 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, i u vrijeme određivanja sredstava obrade i u vrijeme same obrade, provoditi odgovarajuće tehničke i organizacijske mjere za omogućavanje učinkovite primjene načela smanjenja količine podataka. Nadalje, stavkom 2. dodatno je propisano kako se ta obveza primjenjuje na količinu prikupljenih osobnih podataka.

Voditelj obrade je prilikom online transakcija u vidu uplata sredstava na korisnički račun igrača koristio SSL enkripciju - postupak šifriranja podataka koji osigurava prijenos informacija između korisničkog računala i procesora kartica - financijske ustanove certificirane prema PCI DSS Level 1 sigurnosnom standardu propisanom Visa i MasterCard pravilima. Pri čemu voditelj obrade ne pohranjuje potpune podatke o kartici i isti nisu dostupni zaposlenicima voditelja obrade.

Dok se prilikom online transakcija u vidu isplate sredstava sa korisničkog računa na VISA bankovnu karticu financijski podaci obrađuju od strane trinaest zaposlenika bez primjene minimalnih tehničkih mjera u vidu enkripcije podataka u prijenosu /mirovanju i ograničenja pristupa.

Prilikom osmišljavanja procesa obrade voditelj obrade oslonio se na same ispitanike kojima je dao pisanu uputu na koji način prekriti dijelove bankovne kartice da ne dođe do prikupljanja prekomjernog opsega osobnih podataka.

Uputa o načinu prekrivanja pojedinih dijelova kartice koja je uz slikovni primjer dana ispitanicima je neodgovarajuća/ manjkava, iz razloga što je kod većine bankovnih kartica broj kartice utisnut (reljefni), pa se iz toga razloga cjeloviti broj kartice može iščitati s poleđine kartice, a što je i vidljivo iz same obavijesti odnosno slikovnog prikaza iz obavijesti, na kojoj je i na preslici stražnje stranice bankovne kartice vidljiv broj koji je na prikazu prednje strane zatamnjen.

Nakon provedenog nadzora voditelj obrade obavijestio je Agenciju kako je proveo analizu cjelokupnog procesa usluge VISA brze isplate, nakon čega su izvršena dodatna ulaganja u procese plaćanja na način da je sustav unaprijeđen te se u pogledu platnih operacija VISA

karticom primjenjuje 3D Secure - protokol dizajniran da bude dodatni sigurnosni sloj za online transakcije bankovnim i debitnim karticama

Voditelj obrade obvezan je prije nego odredi koje će metode plaćanja ponuditi ispitanicima osigurati da procesi obrade osobnih podataka koje podrazumijevaju odabrane metode plaćanja budu sigurni i zaštićeni od svih predvidivih rizika. U konkretnom slučaju postoji rizik prijevare na štetu ispitanika, a koji može pretrpjeti imovinsku štetu.

Slijedom navedenog, razvidno je kako voditelj obrade, u vrijeme određivanja sredstava obrade vezanih za uslugu VISA brze isplate , nije uzeo u obzir najnovija dostignuća, kao ni visok rizik koju takva obrada može predstavljati za prava i slobode ispitanika te je tek nakon nadzora Agencije proveo analizu procesa te implantirao odgovarajuća sredstva obrade kako bi osigurano jednaku razinu sigurnosti neovisno o tome o radi li se o obradi osobnih podataka u svrhu uplate ili isplate novčanih sredstava.

Sukladno odredbama članka 32. stavak 1. toč. a) i d) Opće uredbe o zaštiti podataka voditelj obrade obvezan je provoditi odgovarajuće tehničke i organizacijske mjere kako bi osigurao odgovarajuću razinu sigurnosti s obzirom na rizik, uključujući između ostalog enkripciju osobnih podataka te provođenje procesa za redovno testiranje, ocjenjivanje i procjenjivanje učinkovitosti tehničkih i organizacijskih mjera za osiguravanje sigurnosti obrade.

Naime, internim aktom voditelja obrade naziva Information classification Policy (hrv. Politika klasifikacije podataka), a koji se odnosi na sve oblike podataka, uključujući tiskane kopije i digitalne podatke pohranjene na bilo kojem mediju ili bilo kojem uređaju i okruženju, definirana su pravila i okvir za klasifikaciju podataka i mjere zaštite na temelju zakonskih zahtjeva kao i osjetljivosti podataka te poslovne vrijednosti podataka.

Sukladno navedenom dokumentu, financijski podaci te osobni podaci korisnika usluga/igrača kategorizirani su kao povjerljivi podaci te je kao odgovarajuća tehnička mjera propisana enkripcija podataka koja se treba primjenjivati pri pohranjivanju elektroničkih dokumenata.

U odnosu na procese redovitog procjenjivanja učinkovitosti tehničkih i organizacijskih mjera za osiguravanje sigurnosti obrade voditelj obrade oslanjao se na obvezu koja proizlazi iz radno-pravne obveze neposrednih rukovoditelja da nadziru rad zaposlenika, a što između ostalog obuhvaća i provođenje interne upute za zaposlenike voditelja obrade naziva „Proces isplate na VISA bankovne kartice“, a kojom je propisano kako je potrebno obrisati nepropisno dostavljene preslike bankovnih kartica od strane ispitanika.

Voditelj obrade je naveo kako provodi tjedne kolegije, nenajavljene kontrole procesa rada te informacija o provođenju radnih obveza, a o čemu se ne sastavlja zapisnik ukoliko nije došlo do povrede koju je nužno dokumentirati te navodi kako je rukovoditelj Sektora korisničkih operacija redovito ustanovljavao kako je postupanje zaposlenika u vezi predmetne obrade bilo usklađeno s propisnima.

Tijekom ovog postupka utvrđeno kako su unutar mape naziva „ “ pohranjene preslike identifikacijskih dokumenata za 27 igrača, kao i preslike bankovnih kartica (VISA, MAESTRO, MASTERCARD) za 2078 igrača, od čega 52 bankovne kartice MAESTRO i MASTERCARD koje uopće nisu podržane uslugom brze VISA isplate, a na 665 pohranjenih preslika bankovnih kartica je vidljiv i verifikacijski broj bankovne kartice u izvornom obliku, na koje nije bio primijenjen algoritam za enkripciju tj. iste nisu bile u kriptiranom formatu.

Slijedom navedenog, u odnosu na obradu osobnih podataka u vidu pohrane podataka igrača u podatkovnom centru voditelja obrade, utvrđeno je kršenje članka 32. stavak 1. toč. a) Opće uredbe o zaštiti podataka, obzirom da je utvrđeno kako voditelj obrade nije primijenio tehničku mjeru zaštite u vidu enkripcije na pohranjene osobne podatke ispitanika a koje su sadržane unutar podmapa u mapi , kao ni tehničku mjeru ograničenja pristupa u vidu lozinke.

Zaključno, utvrđeno je kršenje i članka 32. stavak 1. toč. d) Opće uredbe o zaštiti podataka obzirom da voditelj obrade nije dokazao kako je redovito procjenjivao učinkovitosti tehničkih i organizacijskih mjera za osiguravanje sigurnosti obrade, a što proizlazi iz propusta koje je voditelj obrade propustio utvrditi. Konkretni propusti odnose se na ne provođenja enkripcije, propuštanja implementiranja pristupnih ograničenja bazama podataka unatoč odredbama internih akata o adekvatnim mjerama zaštite.

Nadalje, voditelj obrade propustio je detaljnije urediti proces za redovno testiranje, ocjenjivanje i procjenjivanje učinkovitosti tehničkih i organizacijskih mjera za osiguravanje sigurnosti obrade te se oslonio na organizacijsku mjeru u vidu sistematizacije rada te postupak nadzora ispunjenja radnih obveza, a koje voditelj obrade nije izričito propisao internim aktima. Nadzor, se u konkretnom slučaju sastojao od tjednih kolegija, nenajavljenih kontrola procesa rada te informacija o provođenju radnih obveza. Slijedom čega je utvrđeno da voditelj obrade nije jasno propisao procese nadzora nad obradom osobnih podataka od strane svojih zaposlenika, a kojima bi bili razrađene tehničke i organizacijske mjere koje omogućuju nadzor i praćenje aktivnosti obrade osobnih podataka od strane zaposlenika voditelja obrade.

Drugim riječima, utvrđeno je kršenje članka 32. stavka 1. toč. a) jer je voditelj obrade propustio kriptirati datoteke koje su sadržane u mapi , dok je kršenje članka 32. stavka 1. toč. d) utvrđeno iz razloga što voditelj obrade nije provjeravao da li se internim aktima propisana mjera enkripcije uistinu provodi.

## II. UTVRĐENJE UPRAVNE NOVČANE KAZNE

Člankom 44. Zakona o provedbi Opće uredbe o zaštiti podataka je propisano da Agencija izriče upravne novčane kazne za povrede odredaba ovoga Zakona i Opće uredbe o zaštiti podataka, sukladno članku 83. Opće uredbe o zaštiti podataka.

Člankom 45. stavkom 1. navedenog Zakona je propisano da se upravne novčane kazne izriču odlukom. Temeljem stavka 2. istoga članka, odlukom će se utvrditi iznos i način uplate upravne novčane kazne. Odlukom se može utvrditi da se upravna novčana kazna plaća u obrocima. Temeljem stavka 4. istoga članka, protiv odluke nije dopuštena žalba, ali se može pokrenuti upravni spor pred nadležnim upravnim sudom.

Temeljem članka 46. istoga Zakona, upravna novčana kazna uplaćuje se u roku od 15 dana od dana pravomoćnosti odluke kojom je izrečena. Ako stranka u propisanom roku ne uplati upravnu novčanu kaznu odnosno po dospijeću zadnjeg obroka ako je odobreno obročno plaćanje, Agencija će obavijestiti Područni ured Porezne uprave Ministarstva financija na čijem je području prebivalište odnosno sjedište stranke kojoj je izrečena upravna novčana kazna, radi naplate upravne novčane kazne prisilnim putem prema propisima o prisilnoj naplati poreza. Upravne novčane kazne uplaćuju se u korist državnog proračuna. Iznimno od stavka 2. ovoga članka, na dospjelu, a neplaćenu upravnu novčanu kaznu ne obračunava se kamata.

S obzirom na utvrđene okolnosti u konkretnom slučaju Agencija je sukladno svojim ovlastima iz članka 58. stavka 2. točke (i) Opće uredbe o zaštiti podataka izrekao upravno novčanu kaznu

umjesto drugih korektivnih mjera iz predmetnog članka, a sve u skladu s uvjetima za njezino izricanje iz članka 83. Opće uredbe o zaštiti podataka i članka 44., 45. i 46. Zakona o provedbi Opće uredbe o zaštiti podataka. Nakon detaljnog razmatranja raspoloživih korektivnih mjera iz članka 58. stavka 2. Opće uredbe o zaštiti podataka, a koje nadzorno tijelo ima ovlasti izreći voditelju i/ili izvršitelju obrade, u slučaju kršenja odredbi Opće uredbe o zaštiti podataka, te cijeneći sve okolnosti predmetnog slučaja, a posebno da odabrana korektivna mjera mora biti učinkovita, proporcionalna i odvraćajuća u svakom pojedinom slučaju, Agencija je odlučila izreći upravno novčanu kaznu posvećujući dužnu pozornost kriterijima propisanim člankom 83. stavkom 2. Opće uredbe o zaštiti podataka.

Naime, člankom 83. stavkom 1. Opće uredbe o zaštiti podataka propisano je da svako nadzorno tijelo osigurava da je izricanje upravnih novčanih kazni u skladu s ovim člankom u pogledu kršenja ove Uredbe iz stavaka 4., 5. i 6. u svakom pojedinačnom slučaju učinkovito, proporcionalno i odvraćajuće.

Agencija smatra da iznos izrečene upravne novčane kazne ne može biti učinkovit ako nema značajan utjecaj na prihode voditelja obrade, načelo proporcionalnosti ne može se održati ako se povreda razmatra apstraktno bez obzira na utjecaj na voditelja ili izvršitelja obrade, a ista treba biti i odvraćajuća od budućih kršenja. Dakle, izrečena upravna novčana kazna ne može biti odvraćajuća ako nema financijskog utjecaja na predmetnog voditelja obrade.

Izricanjem upravne novčane kazne ujedno se želi postići da se poštuju pravila o zaštiti osobnih podataka kako od strane samog voditelja obrade tako i od svih drugih voditelja/izvršitelja obrade koji obrađuju osobne podatke u vidu prikupljanja preslike bankovnih kartica sa cjelovitim prikazom podataka na istoj. Izricanjem upravne novčane kazne treba se postići generalno odvraćanje (obeshrabriti druge u ponavljanju istog kršenja u budućnosti), kao i posebno odvraćanje (obeshrabriti adresata ove upravne novčane kazne od ponavljanja istih kršenja).

Sukladno Smjernicama Radne skupine iz članka 29. o primjeni i određivanju upravnih novčanih kazni za potrebe Uredbe 2016/679 od 3. listopada 2017. godine (WP 253), a koje je Europski odbor za zaštitu podataka podržao na svojoj prvoj plenarnoj sjednici 25. svibnja 2018. godine, kako bi se osigurala postojana i visoka razina zaštite pojedinaca te uklonile prepreke protoku osobnih podataka unutar Unije, razina zaštite trebala bi biti jednaka u svim državama članicama (uvodna izjava 10 Opće uredbe o zaštiti podataka). U uvodnoj izjavi 11 pojašnjava se činjenica da su za jednaku razinu zaštite osobnih podataka diljem Unije potrebne, među ostalim, "jednake ovlasti praćenja i osiguravanja poštovanja pravila za zaštitu osobnih podataka i jednake sankcije za kršenja u državama članicama". Nadalje, kako je navedeno u uvodnoj izjavi 13 Opće uredbe o zaštiti podataka, jednake sankcije u svim državama članicama te učinkovita suradnja među nadzornim tijelima različitih država članica potrebni su da bi se "spriječila razilaženja koja ometaju slobodno kretanje osobnih podataka na unutarnjem tržištu".

Temeljem članka 83. stavka 2. Opće uredbe o zaštiti podataka, upravne novčane kazne izriču se uz mjere ili umjesto mjera iz članka 58. stavka 2. točaka od (a) do (h) i članka 58. stavka 2. točke (j), ovisno o okolnostima svakog pojedinog slučaja. Pri odlučivanju o izricanju upravne novčane kazne i odlučivanju o iznosu te upravne novčane kazne u svakom pojedinom slučaju dužna se pozornost posvećuje sljedećem:
(a) prirodi, težini i trajanju kršenja, uzimajući u obzir narav, opseg i svrhu obrade o kojoj je riječ kao i broj ispitanika i razinu štete koju su pretrpjeli;

(b) ima li kršenje obilježje namjere ili nepažnje;
(c) svakoj radnji koju je voditelj obrade ili izvršitelj obrade poduzeo kako bi ublažio štetu koju su pretrpjeli ispitanici;
(d) stupnju odgovornosti voditelja obrade ili izvršitelja obrade uzimajući u obzir tehničke i organizacijske mjere koje su primijenili u skladu s člancima 25. i 32.;
(e) svim relevantnim prijašnjim kršenjima voditelja obrade ili izvršitelja obrade;
(f) stupnju suradnje s nadzornim tijelom kako bi se otklonilo kršenje i ublažili mogući štetni učinci tog kršenja;
(g) kategorijama osobnih podataka na koje kršenje utječe;
(h) načinu na koji je nadzorno tijelo doznalo za kršenje, osobito je li i u kojoj mjeri voditelj obrade ili izvršitelj obrade izvijestio o kršenju;
(i) ako su protiv dotičnog voditelja obrade ili izvršitelja obrade u vezi s istim predmetom prethodno izrečene mjere iz članka 58. stavka 2., poštovanju tih mjera;
(j) poštovanju odobrenih kodeksa ponašanja u skladu s člankom 40. ili odobrenih mehanizama certificiranja u skladu s člankom 42.; i
(k) svim ostalim otegotnim ili olakotnim čimbenicima koji su primjenjivi na okolnosti slučaja, kao što su financijska dobit ostvarena kršenjem ili gubici izbjegnuti, izravno ili neizravno, tim kršenjem.

Nadalje, odredba stavaka 3. istog članka propisuje ako voditelj obrade ili izvršitelj obrade za istu ili povezane obrade namjerno ili iz nepažnje prekrši nekoliko odredaba ove Uredbe ukupan iznos novčane kazne ne smije biti veći od administrativnog iznosa utvrđenog za najteže kršenje.

U članku 83. stavku 4. Opće uredbe o zaštiti podataka je propisano da se za kršenja obveza voditelja i izvršitelja obrade u skladu s člancima 25. i 32. Opće uredbe o zaštiti podataka mogu izreći upravne novčane kazne u iznosu do 10 000 000 EUR, ili u slučaju poduzetnika do 2 % ukupnog godišnjeg prometa na svjetskoj razini za prethodnu financijsku godinu, ovisno o tome što je veće.

U članku 83. stavku 5. Opće uredbe o zaštiti podataka je propisano da se za kršenja obveza voditelja i izvršitelja obrade u skladu s člancima 6. i 13. Opće uredbe o zaštiti podataka mogu izreći upravne novčane kazne u iznosu do 20 000 000 EUR, ili u slučaju poduzetnika do 4 % ukupnog godišnjeg prometa na svjetskoj razini za prethodnu financijsku godinu, ovisno o tome što je veće.

Uvodnom izjavom 150 Opće uredbe o zaštiti podataka navodi se da u slučaju kada se upravne novčane kazne izriču poduzetniku, poduzetnik bi se u te svrhe trebao tumačiti u skladu s člankom 101. i 102. Ugovora o funkcioniranju Europske unije.

Sukladno Smjernicama Radne skupine iz članka 29. o primjeni i određivanju upravnih novčanih kazni za potrebe Uredbe 2016/679 od 3. listopada 2017. godine (WP 253), a koje je Europski odbor za zaštitu podataka podržao na svojoj prvoj plenarnoj sjednici 25. svibnja 2018. godine, kako bi nadzorno tijelo izreklo novčanu kaznu koja je učinkovita, proporcionalna i odvraćajuća, ono primjenjuje definiciju pojma poduzetnika kako ju je naveo Sud Europske unije za potrebe primjene članaka 101. i 102. UFEU-a, to jest smatra se da koncept poduzetnika znači gospodarsku jedinicu koju mogu osnovati matično društvo i sva uključena društva kćeri. U skladu s pravom EU-a i sudskom praksom, pojam poduzetnika treba shvatiti kao gospodarsku jedinicu koja se bavi komercijalnim/gospodarskim djelatnostima bez obzira na uključenu pravnu osobu.

U navedenim Smjernicama navode se i definicije pojma "poduzetnik" iz odluka Suda Europske Unije: Pojam "poduzetnik" obuhvaća svaki subjekt "koji obavlja gospodarsku djelatnost, neovisno o pravnom statusu tog subjekta i načinu njegova financiranja". Pojam poduzetnika "mora se smatrati izrazom kojim se označava gospodarska jedinica čak i ako se u pravu ta gospodarska jedinica sastoji od nekoliko osoba, bilo fizičkih ili pravnih.".

Uvidom u sudski registar utvrđeno je kako je jedini član voditelja obrade - Fortuna Entertainment Group a.s., Češka, Broj iz registra: 141 01 785, 120 00 Praha 2, Italská 2584/69, Vinohrady.

Obzirom da financijsko izvješće za predmetnu grupaciju nije bilo javno dostupno, voditelj obrade dostavio je zatraženo službeno financijsko izvješće za Fortuna Entertainment Group a.s. a čiji je član.

Nadalje, budući da ukupni godišnji promet na svjetskoj razini u 2021. godini za grupaciju Fortuna Entertaiment Group čiji je član društvo Hattrick-PSK d.o.o., iznosi 82.664.000,00 EUR 4% tog iznosa je 3.306.560,00 EUR, odnosno manje od 20.000.000,00 EUR, a koji iznos predstavlja gornju granicu za izricanje upravne novčane kazne u konkretnom predmetu.

Agencija je radi kršenja članaka 6. stavak 1. toč. b) i c), članka 13. stavak 1. i 2., članka 25. stavka 1. i 2. te članka 32. stavka 1. točke a) i d) Opće uredbe o zaštiti osobnih podataka izreko voditelju obrade Hattrick-PSK d.o.o. upravnu novčanu kaznu u iznosu od 380.000,00 EUR a koji iznos čini 1,9 % u odnosu na maksimalni iznos upravne novčane kazne koju je u konkretnom slučaju Agencija mogla, odnosno bila ovlaštena izreći.

Izraz „sa dužnom pozornošću" iz članka 83. stavka 2. Opće uredbe o zaštiti podataka omogućuje nadležnim nadzornim tijelima za zaštitu podataka široku diskreciju prilikom cijenjenja elemenata iz članka 83. stavka 2. Opće uredbe o zaštiti podataka. Agencija je prilikom određivanja visine upravne novčane kazne bila u obvezi poštivati mehanizam konzistentnosti, odnosno osigurati da visina izrečene upravne novčane kazne bude u skladu s kaznama koje su izrekla druga nadzorna tijela za zaštitu podataka drugih država članica Europske unije, u istim odnosno sličnim okolnostima.

Na temelju odredbe članka 83. stavka 2. Opće uredbe o zaštiti podataka, pri odlučivanju o izricanju upravne novčane kazne i odlučivanju o iznosu te upravne novčane kazne, Agencija je u ovom slučaju dužnu pozornost posvetila sljedećem:

- Priroda, težina i trajanje kršenja, uzimajući u obzir narav, opseg i svrhu obrade o kojoj je riječ kao i broj ispitanika i razinu štete koju su pretrpjeli (članak 83. stavak 2, točka a);

U predmetnom slučaju, utvrđeno je kako je voditelj obrade od lipnja do prosinca 2022. godine, nezakonito obrađivao preslike bankovnih kartica primjenom neadekvatnih sredstva obrade, te iste pohranio bez primjene odgovarajućih tehničkih i organizacijskih mjera. Također, voditelj obrade o predmetnoj obradi nije informirao ispitanike sukladno načelu transparentnosti te su na taj način ispitanici bili zakinuti za osnovne informacije o obradi podataka kao što su pravna osnova, svrha i razdoblje pohrane.

Na ozbiljnost ove povrede najbolje ukazuje činjenica kako su zaposlenici voditelja obrade preko 5 mjeseci imali pristup 655 preslika bankovnih kartica na kojima se bio vidljiv pun opseg podataka od ukupno prikupljenih 2078 preslika bankovnih kartica. Naime predmetna obrada

rezultirala je sa visokorizičnom povredom trećine ukupno obrađenih podataka, obzirom da je na trećini preslika bio vidljiv pun opseg podataka. Pri čemu ispitanici nisu bili ni svjesni da se predmetni podaci pohranjuju u bazama podataka voditelja obrade.

Uzimajući u obzir da je predmetna obrada u svrhu isplate dobitka predstavlja osnovnu djelatnost voditelja obrade, Agencija je prethodne okolnosti kvalificirala kao teško kršenje odredaba Opće uredbe o zaštiti podataka.

- Ima li kršenje obilježje namjere ili nepažnje (članak 83. stavak 2, točka b);

Obzirom da su internim pravilnicima voditelja obrade bili predviđeni odgovarajući procesi, tehničke i organizacijske mjere, a koji nisu implementirani u sustav, te da voditelj obrade nije stekao izravnu materijalnu dobit, u predmetnom slučaju nije utvrđena izravna namjera kršenja odredaba Opće uredbe o zaštiti podataka od strane voditelja obrade, već je utvrđena gruba nepažnja.

- Svaka radnja koju je voditelj obrade ili izvršitelj obrade poduzeo kako bi ublažio štetu koju su pretrpjeli ispitanici (članak 83. stavak 2., točka c);

Obzirom da u predmetnom slučaju nije utvrđeno da su ispitanici pretrpjeli štetu ista okolnost nije cijenjena ni kao olakotna ni kao otegotna.

- Stupanj odgovornosti voditelja obrade ili izvršitelja obrade uzimajući u obzir tehničke i organizacijske mjere koje su primijenili u skladu s člancima 25. i 32. (članak 83. stavak 2 točka d);

Kao olakotnu okolnost Agencija je prilikom izricanja upravno novčane kazne posebno cijenila stupanj odgovornosti koji je voditelj obrade pokazao nakon provedenog nadzora od strane Agencije. Naime, voditelj obrade je na svoju inicijativu obavijestio Agenciju o načinu na koji planirala uskladiti predmetnu obradu sa odredbama Opće uredbe o zaštiti podataka te obavijestio o završetku planiranog procesa. Voditelj obrade naveo je kako je proveo analizu cjelokupnog procesa usluge VISA brze isplate, izvršio dodatna ulaganja u procese plaćanja na način da je sustav unaprijeđen, a što podrazumijeva da se od ispitanika više ne traži dostava preslike bankovnih kartica te kako su obrisane sve pohranjene preslike bankovnih kartica. Nadalje, voditelj obrade je naveo je kako je unaprijedio poslovne procese nadzora nad obradom osobnih podataka te educirao zaposlenike.

- Relevantna prijašnja kršenja voditelja obrade ili izvršitelja obrade (članak 83. stavak 2. točka e);

Agencija nije utvrdila prijašnja kršenja odredaba o zaštiti podataka od strane voditelja obrade.

- Stupanj suradnje s nadzornim tijelom kako bi se otklonilo kršenje i ublažili mogući štetni učinci tog kršenja (članak 83. stavak 2. točka f);

Voditelj obrade je tijekom ovog upravnog postupka na odgovarajući način odgovarao na zahtjeve nadzornog tijela, no obzirom da je predmetna okolnost već uzeta u obzir kao olakotna u točki odnosnoj na okolnost iz članak 83. stavak 2 točka d) isto se neće dvostruko vrednovati.

- Kategorije osobnih podataka na koje kršenje utječe (članak 83. stavak 2. točka g);

Financijski podaci ne pripadaju u posebne kategorije osobnih podataka iz članka 9. Opće uredbe o zaštiti podataka. Međutim, sukladno smjernicama izdanim od Europskog odbora za zaštitu podataka financijski podaci smatraju se osjetljivom kategorijom osobnih podataka koji ovisno o kontekstu i opsegu obrade mogu prouzročiti visok rizik za prava i slobode ispitanika te je stoga voditelj obrade bio u obvezi s posebnom pozornošću paziti na sigurnost i zakonitost obrade. Isto je uzeto u obzir kao otegotna okolnost.

- Način na koji je nadzorno tijelo doznalo za kršenje, osobito je li i u kojoj mjeri voditelj obrade ili izvršitelj obrade izvijestio o kršenju (članak 83. stavak 2. točka h);

Za predmetnu povredu nadzorno tijelo je saznalo putem zaprimljenog podneska od strane građana te pokrenulo postupak po službenoj dužnosti. Nadalje, utvrđeno je da voditelj obrade nije zaprimio pritužbe ispitanika odnose na predmetno kršenje.

Nakon pokretanja postupka po službenoj dužnosti, voditelj obrade proveo je cjelokupnu analizu poslovnog procesa te poduzeo adekvatne mjere za usklađivanje postupka obrade s odredbama Opće uredbe o zaštiti podataka. Za pretpostaviti je da je za povredu povjerljivosti podataka voditelj obrade saznao tijekom provedene analize cjelokupnog poslovnog procesa.

U trenutku kada je voditelj obrade postao svjestan povrede povjerljivosti osobnih podataka odnosno neovlaštenog uvida od strane svojih zaposlenika u prekomjerni opseg financijskih podataka, obavijest o povredi bila je suvišna.

Obzirom da je predmetno kršenje odredaba Opće uredbe o zaštiti podataka samo posljedica kršenja članaka 6., 25. i 32., u konkretnom slučaju ova okolnost nije se uzela u obzir prilikom određivanja iznosa upravno novčane kazne.

- Ako su protiv dotičnog voditelja obrade ili izvršitelja obrade u vezi s istim predmetom prethodno izrečene mjere iz članka 58. stavka 2., poštovanju tih mjera (članak 83. stavak 2. točka i);

Obzirom da voditelju obrade nije prethodno izrečena mjera iz članka 58. stavka 2. Opće uredbe o zaštiti podataka, predmetna okolnost nije uzeta u obzir prilikom određivanja iznosa upravno novčane kazne.

- Poštovanje odobrenih kodeksa ponašanja u skladu s člankom 40. ili odobrenih mehanizama certificiranja u skladu s člankom 42. (članak 83. stavak 2. točka j);

Nije relevantno.

- Svi ostali otegotni ili olakotni čimbenici koji su primjenjivi na okolnosti slučaja, kao što su financijska dobit ostvarena kršenjem ili gubici izbjegnuti, izravno ili neizravno, tim kršenjem (članak 83. stavak 2. točka k);
Prilikom određivanja iznosa upravne novčane kazne Agencija nije utvrdila druge relevantne okolnosti koje bi se imale smatrati otegotnima ili olakotnim.

Novčana kazna može se smatrati učinkovitom ako se njome postižu ciljevi zbog kojih je izrečena. To može biti ponovna uspostava poštivanja pravila, kažnjavanje nezakonitog ponašanja ili oboje.

Agencija se odlučila upravo za izricanje upravne novčane kazne kao korektivne mjere iz razloga postojanja visokog rizika za ispitanike, a koji se mogao prevenirati ulaganjem dužne pažnje, dobrog gospodarstvenika. Također, riječ je o voditelju obrade koji je vodeći u djelatnosti kojom se bavi te ima veliki prihod. Isto tako je u predmetnom slučaju došlo do nepotrebnog izlaganja „osjetljivih" osobnih podataka većeg broja ispitanika na način da je određeni broj zaposlenika voditelja obrade bez pretjeranog napora mogao iskoristiti predmetne osobne podatke ispitanika te im nanijeti ozbiljnu materijalnu štetu, a što bi bilo nemoguće ispraviti naknadnim postupanjem voditelja obrade.

Agencija smatra da će izricanje iste dovesti do toga da voditelj obrade pravovremeno ispunjava svoje obveze u području zaštite osobnih podataka u budućnosti, a osobito u pogledu implementiranja odgovarajućih tehničkih i organizacijskih mjere koje omogućavaju učinkovitu primjenu načela zaštite podataka.

Nadalje, imajući na umu da novčana kazna također treba biti razmjerna i odvraćajuća Agencija smatra da izrečena novčana kazna nije nesrazmjerna ciljevima koji se žele postići, te da iznos izrečene novčane kazne razmjeran povredi, pri čemu se posebno vodilo računa o težini povrede te veličini poduzetnika kojem voditelj obrade koji je počinio povredu pripada.

Agencija je provela ispitni postupak sukladno člancima 51. i 52. Zakona o općem upravnom postupku i sukladno svim načelima upravnog postupka propisanih ZUP-om, pravilno utvrdio činjenično stanje te je na temelju utvrđenog činjeničnog stanja pravilno primijenio materijalno pravo i izvela pravilan zaključak o činjeničnom stanju u konkretnom predmetu. Svoju odluku temelji na svim relevantnim dokazima i činjenicama kojima je raspolagao i koje je voditelj obrade dostavio kao dokaze.

Jednako tako, uzimajući u obzir sve prethodno navedeno Agencija smatra da je upravo korektivna mjera u vidu upravne novčane kazne učinkovita, proporcionalna i odvraćajuća u ovoj upravnoj stvari, te da je njezin iznos u potpunosti primjeren okolnostima konkretnog slučaja.

Temeljem svega navedenog 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 Splitu u roku od 30 dana od dana dostave rješenja.

**RAVNATELJ**

**Zdravko Vukić, univ. mag.oec.**

Dostaviti:
1. Hattrick-PSK d.o.o., Ulica sv. Leopolda Mandića 14, 21204 Dugopolje
2. Pismohrana, ovdje