REPUBLIKA HRVATSKA
AGENCIJA ZA ZAŠTITU
OSOBNIH PODATAKA

KLASA: UP/I-034-01/23-01/24
URBROJ: 567-02/11-23-01
Zagreb, 14. rujna 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 (Opća uredba o zaštiti podataka) SL EU L119, članaka 36., 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), a postupajući po službenoj dužnosti protiv voditelja obrade društva X iz _____ OIB: ____ u postupku prava na zaštitu osobnih podataka, donosi sljedeće

R J E Š E NJ E

1. Utvrđuje se da je društvo X iz _____ kao voditelj obrade obrađivalo osobne podatke ispitanika u prekomjernom opsegu u vidu podataka sigurnosnog broja bankovne kartice, odnosno CVC/CVV broja, kao i preslike osobnih dokumenta prilikom rezervacije smještaja X putem online obrasca Webbookingpro i putem e-pošte koju koristi X za čiju obradu osobnih podataka nije dokazano postojanje pravne osnove, a čime je povrijeđen članak 6. stavak 1. Opće uredbe o zaštiti podataka.

2. Utvrđuje se da društvo X iz ___ kao voditelj obrade nije na jasan/transparentan način informiralo ispitanike o obradi njihovih osobnih podataka putem dokumenta *Opći uvjeti poslovanja - X*, koji je dostupan na mrežnim (web) stranicama X, a u pogledu prikupljanja osobnih podataka prilikom rezervacije smještaja Hotela putem online obrasca Webbookingpro i putem e- pošte, a što je protivno odredbi članka 13. stavka 1. i 2. Opće uredbe o zaštiti podataka.

3. Utvrđuje se da je društvo X iz _____, kao voditelj obrade prilikom slanja obrasca *„Privola na korištenje osobnih podataka"* u svrhu pružanja informacija ispitanicima o obradi njihovih osobnih podataka prilikom rezervacije smještaja hotela putem e-pošte, a koji obrazac ne sadrži točne ni cjelovite informacije, postupilo protivno odredbama članka 13. stavka 1. i 2. Opće uredbe o zaštiti podataka.

4. Utvrđuje se da je ne poduzimanjem odgovarajućih organizacijskih i tehničkih mjera zaštite kod obrade osobnih podataka ispitanika od strane društva X iz ____, kao voditelja obrade došlo do povrede članka 32. stavka 1. a) i d) i članka 32. stavka 4. Opće uredbe o zaštiti podataka.

5. Utvrđuje se da je društvo X iz ___, kao voditelj obrade imenovalo voditelja Y iz _____ OIB: _____ službenikom za zaštitu podataka X protivno odredbama članka 38. stavka 6. Opće uredbe o zaštiti podataka.

6. Za kršenja opisana u točkama 1. - 5. izreke ovog rješenja, u skladu s odredbama članka 83. Opće uredbe o zaštiti podataka, izriče se društvu X iz ___, kao voditelju obrade upravna novčana kazna u iznosu od:

15.000, 00 EUR/ 113.017,50 kn[1]

(slovima: petnaest tisuća eura/sto trinaest tisuća sedamnaest kuna i pedeset lipa)

Društvo X iz __, kao voditelj obrade 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: 6092-25860-25114795185 s naznakom – "upravne novčane kazne koje izriče AZOP".

7. Ukoliko društvo X iz ___, kao voditelj obrade 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.

8. Društvo X iz __, kao voditelj obrade je dužno u roku od 15 dana od izvršene uplate dostaviti dokaz o uplati Agenciji za zaštitu osobnih podataka.

O b r a z l o ž e nj e

I. UTVRĐENJE POVREDE

Agencija za zaštitu osobnih podataka (dalje u tekstu: Agencija) zaprimila je dana 27. veljače 2023. godine podnesak građanina u kojem se u bitnome navodi kako se na lokaciji Hotela X (dalje u tekstu: hotel) na adresi ____ voditelja obrade društva X iz _____(dalje u tekstu: društvo) prilikom rezervacije smještaja traži potvrda rezervacije slanjem broja kreditne kartice (putem obrasca) i to potpuno nezaštićenim kanalima (putem elektroničke pošte). Isto tako, u zaprimljenom podnesku se navodi kako potencijalni gost nije upoznat/informiran tko ima

[1] Fiksni tečaj konverzije 7,53450 kn

pristup njegovim osobnim podacima, točnije osobnom dokumentu koji je isti na traženje dužan poslati (osobna iskaznica, putovnica, vozačka dozvola), a sve kako bi se mogla teretiti kreditna kartica.

U tijeku postupka Agencija je dana 05. travnja 2023. godine provela izravne nadzorne aktivnosti na lokaciji X o čemu je kao dokaz u provedenom postupku sastavljen Zapisnik KLASA: 042-02/23-01/17, URBROJ: 567-12/09-23-05 od 13. travnja 2023. godine.

Nadzornim aktivnostima od strane Agencije je utvrđeno da je Y od 1. siječnja 2022. voditelj X kao i službenik za zaštitu podataka društva X unutar kojeg i posluje predmetni Hotel.

U odnosu na obradu osobnih podataka koju provodi predmetni voditelj obrade unutar poslovanja Hotela X, u tijeku nadzornih aktivnosti Y, navodi da su isti u obvezi poradi poštivanja pravne obveze iz Zakona o turističkoj pristojbi i podzakonskih akata donesenih na temelju navedenog Zakona, od turista odnosno gostiju prikupljati određeni opseg osobnih podataka koji se unosi u sustav eVisitor, a da je navedeni opseg osobnih podatak koji se u tu svrhu prikuplja sadržan i u odredbama akta Opći uvjeti poslovanja Hotel X, u kojem dokumentu se u poglavlju odnosnom na zaštitu osobnih podataka ispitanicima pružaju sve informacije odnosne na obradu osobnih podataka.

U odnosu na gore navedeno, Y ovlaštenim službenicima Agencije prilikom provođenja nadzornih aktivnosti dostavlja Opće uvjete poslovanja X (prethodno preuzete sa mrežne stranice X). S tim u vezi, Y potvrđuje da se radi o aktu X kojim se pružaju informacije ispitanicima, a na upit vezano za opseg podataka sadržan u članku 36. Općih uvjeta poslovanja X, isti navodi kako se prikupljaju osobni podaci ime i prezime, mjesto, država i datum rođenja, državljanstvo, vrsta i broj isprave o identitetu, prebivalište i adresa, datum i vrijeme dolaska i odlaska iz objekta i predviđeni datum odlaska iz objekta, spol, adresa e-pošte i broj telefona, a sve sukladno Pravilniku o sustavu eVistor. Nadalje, u odnosu na osobne podatke koje navode da prikupljaju, a nisu sadržani u Pravilniku o sustavu eVisitor, adresa e-pošte i broj telefona, Y navodi da su im isti nužni poradi izvršenja ugovora o rezervaciji i opcionalno je koji podatak se od ponuđenog dostavi. U odnosu na način prikupljanja osobnih podataka, Y navodi da gost može direktno na recepciji kod dolaska u Hotel pružiti te podatke, nadalje navodi kako se rezervacija može potvrditi i putem pružatelja usluga posredništva tipa Booking.com, Expedia, a tako i putem online obrasca dostupnog na Web stranici Hotela ili putem e-pošte.

Vezano za rezervaciju putem pružatelja usluga, osnovne podatke o gostu, Hotel zaprimi u obavijesti od tog pružatelja usluge, a sam gost tom pružatelju usluge dostavlja osobne podatke kao i podatke za plaćanje njihove usluge. S tim u vezi, Hotel se za pruženu uslugu naplaćuje od tog pružatelja usluge, a ne od gosta, pa stoga Hotel direktno ne prikuplja podatke za plaćanje od gosta, već samo podatke nužne za unos u sustav e-Visitor i to po dolasku gosta u Hotel.

Nadalje, nadzornim aktivnostima Agencije utvrđeno je kako je drugi način rezervacije online rezervacija putem web obrasca, tj. servisa pružatelja usluge Webbookingpro na Internet stranici Hotela. Utvrđeno je kako je kod korištenja tog načina rezervacije potrebno popuniti web obrazac sa osobnim podacima gosta/korisnika i to ime, prezime, adresa e-pošte, poštanska adresa (poštanski broj, grad, država), broj telefona, te financijske podatke u vidu odabira metode plaćanja karticom - tip kartice (Visa, Mastercard, Maestro, Diners, American Express),

broj kartice, datum i godina do kada vrijedi kartica, CVV broj, ime nositelja/vlasnika kartice. Također, na kraju se prikazuje obavijest koju je potrebno prihvatiti čime se ispitanik slaže sa općim uvjetima poslovanja Hotela i kliknuti na potvrdu rezervacije (CONFIRM RESERVATION).

Tijekom nadzornih aktivnosti ovlašteni službenici Agencije izvršili su uvid u sam način online rezervacije na način da je Y putem svog mobilnog uređaja na web stranici Hotela, ispunio sve tražene podatke u WEB obrazac, ali nije unio CVV broj te stoga rezervaciju nije bilo moguće napraviti (ispisala se poruka „No CVV provided! Please re-enter.“). Nakon toga, Y je upisao CVV broj sa tri znamenke, ali proizvoljno (broj 999), što nije točan broj CVV sa njegove kartice i online rezervacija je uspješno izvršena.

Izvršenom provjerom na računalo na recepciji Hotela, u sustavu Webbookingpro koji Hotel koristi za zaprimanje rezervacija, budući da se u konkretnom slučaju radi o online rezervaciji, prikazala se prethodno navedena, stvorena i opisana rezervacija koja sadržava podatke o korisniku/gostu, usluzi, trajanju, ali dio koji se odnosi na financijske podatke (kartici) - „*VIEW CC INFO*“ je bio dodatno zaštićen lozinkom (passwordom), bez unosa koje pristup opisanom nije moguć. Nakon što je Y na računalu na recepciji unio lozinku (password) na predviđeno mjesto prikazuju se podaci: ime nositelja/vlasnika kartice, broj kartice, datum do kada vrijedi kartica, ali nije prikazan tip kartice ni CVV broj. Također, na adresu e-pošte _____ dolaze dva odvojena e-maila. U jednom e-mailu se navodi rezervacija sa šifrom/ID rezervacije i podacima gosta/korisnika, usluzi i vremenu korištenja iste, dok se u drugom e-mailu dostavlja podatak o CVV broju uz naznaku šifre/ID rezervacije kao naslovu e-maila.

Nadalje, na izravan upit ovlaštenih službenika Agencije o pohrani podataka koji se prikupljaju putem online rezervacije sustava Webbookingpro Y navodi kako nije siguran, ali da misli da se isti pohranjuju u oblaku kod tvrtke kod koje su ugovorili sustav Webbookingpro.

Također, nadzornim aktivnostima utvrđeno je kako je treći način rezervacije putem e-pošte, te se u tom slučaju kada se zaprimi upit gosta o dostupnosti smještaja, istome šalje na adresu e-pošte sa koje se isti javlja, obrazac koji je potrebno popuniti. Predmetni obrazac sadrži sljedeće osobne podatke ime i prezime, adresa i grad, država, broj osobne iskaznice, datum i godina rođenja, iznos terećenja kreditne kartice, podatak o kreditnoj kartici (vrsta kartice, puno ime vlasnika kartice, broj kartice, datum isteka kartice, CVC).Također, utvrđeno je kako se putem predmetnog obrasca od ispitanika čiji se podaci prikupljaju traži dostava valjanog dokumenta sa fotografijom (osobna iskaznica, putovnica, vozačka dozvola), a sve iz razloga da se može teretiti kreditna kartica.

U tijeku nadzora, ovlašteni službenici Agencije izvršili su uvid u servis Outlook, konkretno adresu e-pošte _____ te je izvršen pregled/pretraga mapa Inbox, Trash, Archive. U mapi Inbox prva dostupna e-poruka je od datuma 02.01.2023., u mapi Trash je prva dostupna e-poruka je od datuma 01.04.2023., a u mapi Archive prva dostupna e-poruka je od datuma 31.08.2022. Pregledom navedenih mapa nisu pronađeni drugi financijski podaci, identifikacijski dokumenti, osim preslike bankovne kartice Z nositelja ZY, zatim obostrana preslika osobne iskaznice istog, ispunjen obrazac privole na korištenje osobnih podataka, obrazac za prikupljanje podataka na kojemu je djelomično vidljiv broj kartice (dva puta po četiri

znamenke, ali uz razmak između znamenki) i CVC broj naznaka telefonom, a na preslici bankovne kartice isti nije vidljiv. Na upit u svezi dostupnosti navedenih podataka A voditeljica recepcije Hotela navodi da su ti podaci još dostupni jer je tek izvršena rezervacije, a nije realizirana usluga smještaja te da će biti isto obrisano po realizaciji usluge.

Na izravni upit ovlaštenih službenika Agencije o nužnosti prikupljanja CVV broja, koji broj se u obrascu označava kao CVC, Y navodi da mu razlog za takav upis naziva nije poznat, te da mu nije poznato da li je isti nužan za provođenje same naplate neotkazane rezervacije, obzirom da isto nije provedeno. Također, Y navodi kako je obrazac sačinjen ranije te da se i dalje koristi.

Dodatno u odnosu na opseg osobnih podataka koji je sadržan na priloženom obrascu, Y navodi da je isti nužan u svrhu potvrde rezervacije, obzirom na mogućnost nastupa štete za Hotel, koji rezervira smještajne kapacitete i u slučaju ne dolaska gosta u rezervirani smještaj nije u mogućnosti pravovremeno popuniti otkazane kapacitete. Ujedno navodi da im pravna osnova za prikupljanje opisanih podataka ugovor, obzirom da smatra da su podaci u opisanom opsegu nužni za naplatu. U svezi sadržane upute na obrascu da je istome potrebno priložiti i presliku identifikacijskog dokumenta Y navodi da je isto nužno prikupiti poradi sprečavanja zlouporaba i kao pravnu osnovu navodi da je isto nužno poradi izvršenja ugovora, s obzirom da i sve radnje oko rezervacija ili otkazivanja iste su dio pružanja usluge smještaja.

Na upit iz kojeg razloga u dokumentu Opći uvjeti poslovanja X nema sadržanih uputa/informacija o prikupljanju i financijskih podataka ni preslika identifikacijskih dokumenata Y navodi da je to iz razloga što se taj obrazac ne odnosi na rezervacije putem e-pošte. Na dodatni upit na koji su način u tom situacijama izvješteni ispitanici o obradi njihovih osobnih podataka Y navodi da se njima šalje obrazac Privole koji sadrži podatak o obradi osobni podataka, a koji obrazac se daje svakom gostu kada fizički dođe u Hotel ali i šalje putem e-pošte uz ranije priloženi obrazac.

U odnosu na sadržaj priloženog obrasca Privole u kojemu se navodi da je pravna osnova obrade osobnih podataka gostiju Hotela privola, koja se daje u svrhu sklapanja i ispunjenja ugovora o smještaju, ispunjenja zakona, zaštite imovine videonadzorom i dr., Y navodi da je prije otvaranja samog Hotela, odvjetničko društvo koje je provelo usklađenje poslovanja Hotela sa odredbama Opće uredbe o zaštiti podataka, sačinilo obrasce i akte odnosne na obradu osobnih podataka te da se isti naknadno nisu revidirali pa su iz tog razloga navedene neujednačenosti. Ujedno navodi da mu je poznato da predmetno odvjetničko društvo koje je provelo usklađenje sačinilo i dodatne akte, ali kako je isto odloženo u registrator te se vjerojatno nalazi na adresi sjedišta društva ili u knjigovodstvu, isto mu nije trenutno dostupno za predati na uvid ovlaštenim službenicima Agencije, a nije mu ni poznat sadržaj navedenog registratora.

Nadalje, Y, u tijeku nadzornih aktivnosti navodi da se navedeni obrasci za potvrdu rezervacije smještaja zaprimaju na adresu e-pošte _____ nakon čega djelatnik na recepciji, nakon što otvori predmetnu poruku e-poštu ispisuje priložene obrasce i pohranjuje ih u fizičkom obliku u registrator gdje se odlažu izlazni računi i rezervacije za smještaj. Po izvršenoj usluzi poruka dostavljena putem e-pošte se briše sa sandučića, a kod same naplate usluge ranije prikupljeni obrazac i preslike dokumenata se fizički uništavaju i u registrator se pohranjuje račun i slip ukoliko je plaćanje bilo putem kartice. U odnosu na navedeno Y navodi da nema dodatnih

internih akata ili uputa zaposlenicima, već da su sve upute dane usmeno. Navodi da zaposlenici nisu potpisali izjave o povjerljivosti već da su obvezani povjerljivošću unutar obveza iz Ugovora o radu koji se potpisuje kod zapošljavanja pojedinog zaposlenika.

Dodatno u tijeku provođenja nadzornih aktivnosti Y prilaže i interni akt, za koji navodi da je sa ostalim informacijama dostupan gostima na recepciji u kojima su opisane svrha i pravna osnova za obradu osobnih podataka uz druge podatke koje je o obradi osobnih podataka potrebno pružiti ispitanicima.

Na upit ovlaštenih službenika Agencije u odnosu na sadržaj internog akta iz kojeg ne proizlazi da predmetni obrazac sadržava informacije o prikupljanju i obradi preslika identifikacijskih podataka kao ni podataka o bankovnim karticama uključivo i podatak o CVV broju Y navodi da je informacija pružena samo unutar obrasca Privole.

Također, na upit Y navodi da koliko mu je poznato do sada nije bio niti jedan slučaj naplate za neotkazanu rezervaciju dogovorenu putem e-pošte, a u svezi čega se i prikupljaju opisani obrasci na kojima su sadržani osobni podaci. Isto tako pojašnjava da se ti obrasci uglavnom i rijetko zaprimaju te se po realizaciji usluge odmah kod postupka izdavanja računa uništavaju, stoga istih nema ni pohranjenih ni u sandučiću e-pošte ni u fizičkoj pohrani dokumenta. U odnosu na broj takvih rezervacija Y navodi da se radi o iznimnim situacijama možda tijekom ljetne sezone, te da se nakon plaćanja usluge unište obrasci i obriše e- mail korespondencija, te stoga nema načina provjere samog broja takvih slučajeva u ranijem periodu.

Nadalje, Y, u odnosu na vrijeme pohrane podataka, navodi da se osobni podaci sadržani u sustavu Milenij pohranjuju 5 godina, kao i podaci o izlaznim računima sukladno propisu iz domene knjigovodstva. Isto tako navodi kako osim u sustav e-Visitor i sustav Milenij ne upisuju osobne podatke gostiju te da se još uvijek čuvaju prikupljani podaci budući da Hotel posluje od travnja 2019. godine.

Nadalje, Z navodi da je unazad 2 godine zaposlena u predmetnom Hotelu i sada je na radnom mjestu voditelja recepcije, te da uz kolege _____ima pristup adresama e-pošte koje koristi predmetni Hotel. Navodi da je lozinka za opisane adrese e-pošte poznata samo njima i Y, ali da isti nemaju zasebne lozinke, s obzirom da se istima pristupa samo sa računala na recepciji. Navodi da su joj sve upute za rad i u odnosu na zaštitu osobnih podataka dane usmeno, da nije potpisivala izjavu o povjerljivosti niti je bila polaznik zasebne edukacije u odnosu na zaštitu osobnih podataka.

Na objašnjenje Y da se dokumentacija o rezervaciji putem e-pošte od zaprimanja do realizacije usluge pohranjuje uz izlazne račune u registratore, ovlašteni službenici Agencije provode pregled nasumično odabranih registratora iz arhive, koja prostorija je zaključana, a u kojim registratorima se odlažu računi, ponude, izvodi banke, obavijesti pružatelja usluga, slipovi o plaćanju i privole o obradi osobnih podataka. S tim u vezi, pregledan je registrator sa sadržanim navedenim dokumentima od 02.12. do 29.12.22., od 14.7. do 24.7. 2022., te se u istima ne pronalaze preslike identifikacijskih dokumenata ni obrazac za prikupljanje podataka o identitetu i podataka o bankovnim karticama. Nadalje, u registratoru u koji se ulažu tekući obrasci, koji se nalaze unutar prostora recepcije, na polici ispod radnog stola, za period od 17.3. do 5.4.2023. pronalazi se unutar pružanja usluge društvu XX preslika poslovne bankovne

kartice XX nositelja XR, preslike osobne iskaznice, ispunjen obrazac privole na korištenje osobnih podataka, obrazac za prikupljanje podataka na kojemu je vidljivo uz broj kartice i CVC broj naznaka telefonom. Provjerom u sandučiću e-pošte vidljivo je da nije upisan CVV broj. S tim u vezi, Z pojašnjava da je kontaktirala navedenog gosta te nakon ispisa rukom upisala podatke kojih nije bilo, a da je isti obrazac i preslika dokumenta sadržana jer je usluga u tijeku te navodi kako će se nakon završetka usluge smještaja isto uništiti u rezaču a i obrisati iz sandučića e-pošte.

Agencija je u svrhu točnog i potpunog činjeničnog stanja dopisom KLASA: 004-02/23-01/177, URBROJ: 567-02/14-23-05 dana 07. lipnja 2023. godine od društva X zatražila dopunu budući da tijekom nadzornih aktivnosti Y navodi kako je voditelj Hotela X te ujedno imenovani službenik za zaštitu podataka društva X o čemu je priložen obrazac Izvješće o imenovanju službenika za zaštitu podataka od 01. siječnja 2022. godine. Također, u provedenom postupku društvo X je naknadno, nakon provedenih nadzornih aktivnosti dostavilo Agenciji dodatne informacije i dokumentaciju, između ostalog, presliku Ugovora o radu na neodređeno vrijeme sklopljenog između društva X i Y od 30. prosinca 2021. godine. Uvidom u navedeni ugovor razvidno je da je u istome ugovoreno kako Y kao radnik obavlja poslove voditelja Hotela.

S obzirom na navedeno, Agencija je od društva X kao voditelja obrade zatražila da pojasni koje poslove (opis radnog mjesta voditelja Hotela) obavlja Y kao voditelj Hotela, temeljem sklopljenog ugovora o radu na neodređeno vrijeme s Hotelom kao poslodavcem, a sve iz razloga što iz dostavljenog ugovora o radu nije razvidno koje sve poslove isti obavlja.

Agencija je dana 23. lipnja 2023. godine zaprimila dopunu od društva X u kojem isto dostavlja Izjavu o dogovorenim zaduženjima i poslovima za zaposlenika Y. U navedenoj Izjavi se navodi kako je prilikom sklapanja ugovora o radu sa Y 30.12.2021. godine dogovoreno da isti obavlja poslove voditelja X i to sa sljedećim zaduženjima: vođenje prodaje hotelskih kapaciteta; direktan rad s predstavnicima putničkih agencija; komunikacija s direktorom društva; podnošenje izvještaja direktoru društva; davanje informacija potrebnih za vođenje društva na direktorov zahtjeva; koordinacija između odjela X; sastavljanje rasporeda rada svih zaposlenika X te komunikacija s gostima X po pritužbama.

Također, Agencija je od društva X kao voditelja obrade zatražila očitovanje/informacije o broju ispitanika, kao fizičkih osoba koju su zatražile od Hotela rezervaciju smještajne jedinice putem servisa pružatelja usluge Webbookingpro na mrežnoj stranci Hotela (online rezervacija) te putem e-pošte, u periodu od travnja 2019. godine od kada Hotel posluje do dana zaprimanja istog dopisa Agencije. Također, od predmetnog društva zatraženo je da dostavi informaciju o ukupnom broju ispitanika, kao fizičkih osoba koje su u gore navedenom periodu koristile uslugu smještaja Hotela.

U vezi s navedenim, Agencija je zaprimila dopis društva X kao voditelja obrade, kojim isto traži produljenje roka za dostavu očitovanja, budući da dostava traženih informacija predstavlja zahtjevan posao jer se traženi podaci vezani uz garancije plaćanja za tražene rezervacije pravovremeno uništavaju i ne čuvaju. Slijedom navedenog, nastavno na traženje društva X odobreno je produljenje roka (do zaključno 04. kolovoza 2023. godine).

U dostavljenom očitovanju društvo X dostavlja listu rezervacija napravljenih putem sučelja Wbbookingpro te listu rezervacija koju su koristili obrasci za autorizaciju kreditnih kartica. S tim u vezi, predmetno društvo navodi kako se osiguranje dolaska i naplate rezervacije putem Obrasca za autorizaciju kreditne kartice koristilo rijetko i to samo u slučaju kada bi gost izričito tražio takav način garancije jer nije htio rezervirati sobu preko neke od partnerskih agencija, putem sučelja Webbookingpro ili nije htio transakcijski avansno uplatiti dio ili punio iznos rezervacije. Također, predmetno društvo uz očitovanje dostavlja akte vezane za uređenje zaštite osobnih podataka, unutar predmetnog voditelja obrade.

Nastavno na navedeno, ističemo kako se od 25. svibnja 2018., u svim državama članicama Europske unije, pa tako i u Republici Hrvatskoj, u području zaštite osobnih podataka 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 119, a za čiju primjenu i provođenje na području Republike Hrvatske je nadležna Agencija za zaštitu osobnih podataka.

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.

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.

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.

Stavak 4. istog članka Opće uredbe o zaštiti podataka propisuje kako voditelj obrade i izvršitelj obrade poduzimaju mjere kako bi osigurali da svaki pojedinac koji djeluje pod odgovornošću voditelja obrade ili izvršitelja obrade, a koji ima pristup osobnim podacima, ne obrađuje te podatke ako to nije prema uputama voditelja obrade, osim ako je to obvezan učiniti prema pravu Unije ili pravu države članice.

Članak 38. stavak 1. Opće uredbe o zaštiti podataka propisuje kako voditelj obrade i izvršitelj obrade osiguravaju da je službenik za zaštitu podataka na primjeren način i pravodobno uključen u sva pitanja u pogledu zaštite osobnih podataka. Stavak 6. istog članka Opće uredbe o zaštiti podataka propisuje kako službenik za zaštitu podataka može ispunjavati i druge zadaće i dužnosti. Voditelj obrade ili izvršitelj obrade osigurava da takve zadaće i dužnosti ne dovedu do sukoba interesa.

Zakon o turističkoj pristojbi („Narodne novine“, broj: 52/19, 32/20, 42/20) propisuje kako su pravna osoba i fizička osoba obrtnik koje pružaju uslugu noćenja u smještajnom objektu ili uslugu noćenja na plovnom objektu nautičkog turizma i osoba koja pruža ugostiteljsku uslugu smještaja u domaćinstvu ili na obiteljskom poljoprivrednom gospodarstvu obvezne su u roku od 24 sata od dolaska prijaviti u sustav eVisitor sve osobe kojima pružaju uslugu noćenja te u roku od 24 sata od odlaska odjaviti njihov boravak (članak 22. stavak 1. Zakona).

Člankom 22. stavkom 10. citiranog Zakona propisano je kako način prijave i odjave turista putem sustava eVisitor, podatke potrebne za prijavu/odjavu te način njihova utvrđivanja, prikupljanja i čuvanja ministar propisuje pravilnikom.

Prema članku 4. Pravilnika o sustavu e-Vistora („Narodne novine“, broj: 43/2020) u popis turista upisuju se sljedeći podaci o turistima: prezime i ime, mjesto, država i datum rođenja, državljanstvo, vrsta i broj isprave o identitetu, prebivalište (boravište) i adresa, datum i vrijeme dolaska u objekt, predviđeni datum odlaska iz objekta, datum i vrijeme odlaska iz objekta, spol, napomena, broj prijave.

Slijedom navedenog, u ovoj upravnoj stvari utvrđeno je kako društvo X obrađuje u određenom opsegu osobne podatke ispitanika prilikom postupka rezervacije smještajne jedinice Hotela putem servisa pružatelja usluge Webbookingpro na mrežnoj stranci Hotela (online rezervacija). Navedenim načinom rezervacije smještajne jedinice Hotela predmetno društvo od ispitanika prikuplja osobne podatke u opsegu imena, prezimena, adrese e-pošte, poštanske adrese (poštanski broj, grad, država), broja telefona, financijske podatke u vidu odabira metode plaćanja bankovnom karticom (tip kartice), broj kartice, datum i godina do kada vrijedi kartica, CVV broj te ime nositelja/vlasnika kartice.

Također, u provedenom postupku je utvrđeno kako je ispitanicima dana mogućnost da izvrše rezervaciju smještajne jedinice Hotela elektroničkim putem (putem e-pošte) i to na način da se ispitaniku na e-poštu sa koje se obratio Hotelu dostavi *Obrazac* koji je isti dužan popuniti svojim osobnim podacima i poslati nazad hotelu putem e-pošte. Isto tako, u postupku je utvrđeno da se predmetnim *Obrascem* prikupljaju osobni podaci ispitanika u opsegu imena i prezimena, adrese i grada, države, broja osobne iskaznice, datuma i godine rođenja, iznosu terećenja kreditne kartice, podatke o kreditnoj kartici (vrsta kartice, puno ime vlasnika bankovne kartice, broj kartice, datum isteka kartice, CVC).

Osim navedenog, u postupku je utvrđeno kako se putem predmetnog *Obrasca* od ispitanika čiji se podaci prikupljaju traži dostava preslike valjanog dokumenta sa fotografijom (osobna iskaznica, putovnica, vozačka dozvola), a sve iz razloga da se može teretiti njegova kreditna kartica. Osim navedenog, uz obrazac se dostavlja i obrazac *Privola na korištenje osobnih podataka* u vidu pružanja informacija ispitanicima o obradi osobnih podataka u postupku gore opisanog načina traženja rezervacije smještajne jedinice Hotela.

Slijedom svega gore navedenog, a s obzirom da je u tijeku provođenja postupka utvrđeno da predmetno društvo prikuplja određeni set/opseg osobnih podataka prilikom postupka rezervacije smještajne jedinice Hotela putem servisa pružatelja usluge Webbookingpro (online rezervacija) te putem e-pošte, a koji, između ostaloga, sadržavaju i podatak o CVC broju (sigurnosnom kontrolnom broju) bankovne kartice ispitanika koji u smislu članka 4. Opće uredbe o zaštiti podataka, posebice u kombinaciji s brojem bankovne kartice predstavlja osobni podatak, odnosno financijski podatak ispitanika za opisanu obradu predmetno društvo mora dokazati postojanje relevantne pravne osnove iz članka 6. stavka 1. Opće uredbe o zaštiti podataka.

Imajući u vidu gore navedenu obvezu predmetnog društva koja proizlazi iz propisa kojima je regulirana zaštita osobnih podataka, a također u odnosu na utvrđeno postupanje od strane predmetnog društva u provedenom postupku od strane ove Agencije, proizlazi kako je opisano postupanje predmetnog društva protivno odredbama članka 6. stavka 1. Opće uredbe o zaštiti podataka. S tim u vezi, navodimo kako je u provedenom postupku uzeta u obzir činjenica da predmetno društvo u opisanom slučaju nije imalo obvezu prikupljanja CVC broja ispitanik koji su izvršili rezervaciju smještajne jedinice Hotela, budući da je rezervacija bila moguća i bez dostavljanja podataka o CVC broju.

S obzirom da predmetno društvo nije dokazalo da je prikupljanje podataka o CVC broju nužan podatak za rezervaciju smještajne jedinice Hotela, navodimo kako je predmetno društvo prilikom pružanja svoje usluge moglo birati manje invazivnu metodu kod obrade osobnih podataka ispitanika/osoba koje traže rezervaciju smještajne jedinice Hotela, pritom vodeći računa da s jedne strane zadovolji kriterije za zakonitu obradu osobnih podataka kako to nalažu odredbe Opće uredbe o zaštiti podataka i drugi posebni propisi, a sa druge strane da omogući traženu uslugu ispitaniku (rezervacija smještajne jedinice Hotela).

Kao bitno navodimo kako je u postupku utvrđeno da predmetno društvo prikuplja određeni set osobnih podatka ispitanika sukladno Zakonu o boravišnoj pristojbi te Pravilniku o sustavu e-

Vistor. Tako, Zakon o sustavu e-Vistor propisuje kako se u Popis turista upisuju podaci o turistima u opsegu prezimena i imena, mjesta, države i datuma rođenja, državljanstva, vrste i broja isprave o identitetu, prebivališta (boravišta) i adrese, datuma i vremena dolaska u objekt, predviđenog datuma odlaska iz objekta, datuma i vremena odlaska iz objekta, spol, napomena te broj prijave.

Stoga imajući u vidu odredbe gore citiranog Pravilnika navodimo kako ne nalazimo uporište za obradu spornih osobnih podataka u odredbama citiranog Pravilnika koji propisuje način prijave i odjave turista putem sustava e-Visitor, podatke potrebne za prijavu/odjavu, te način njihova utvrđivanja, prikupljanja i čuvanja. Dakle, osobito bitnim navodimo kako gore spomenuti Pravilnik ne propisuje obvezu prikupljanja bankovnih podataka, posebice podataka o CVC broju, a tako niti preslike osobnog dokumenta, već obvezu prikupljanja drugog seta osobnih podataka gostiju/turista.

Vezano za prikupljanje preslika dokumenta ispitanika (osobna iskaznica, putovnica, vozačka dozvola) prilikom rezervacije smještaja Hotela, a u svrhu terećenja bankovne kartice, navodimo kako, s aspekta pravnog okvira zaštite osobnih podataka, za prikupljanje preslika osobnih dokumenta koji sadrže osobne podatke ne nalazimo valjanu pravnu osnovu u smislu članka 6. Opće uredbe o zaštiti podataka.

Dakle, predmetno društvo bilo je dužno prepoznati da takvim postupanjem prikuplja veći opseg osobnih podataka ispitanika, a koji nije nužan za konkretnu svrhu.

Nadalje, u postupku je utvrđeno kako se na internetskim stranicama predmetnog društva nalazi dokument *Opći uvjeti poslovanja – X* koji se primjenjuje na pružanje usluga predmetnog društva te uvjete plaćanja i otkazivanja u vezi s rezervacijama koje je izvršio klijent, kao i svim drugim pravima i obvezama koje proizlaze iz pravnog odnosa uspostavljenog korištenjem.

Uvidom u predmetni dokument *Opći uvjeti poslovanja - X* razvidno je kako isti sadrži dio odnosan na *„Zaštitu osobnih podataka i privatnost“*, a koji u članku 35. sadrži informaciju o svrsi prikupljanja osobnih podataka njihovih korisnika (svrha rezervacija smještaja) i obvezi vođenja popisa turista sukladno Pravilniku o sustavu e-Visitor.

Također, u daljnjim člancima *Opći uvjeti poslovanja - X* razrađuje se set/opseg osobnih podataka koji se prikupljaju u gore navedenu svrhu iz članka 35., međutim u istom se ne navodi podatak o CVC broju ispitanika. Isto tako, *Općim uvjetima poslovanja - X* nabrojana su neka od prava ispitanika koja mu pripadaju sukladno Općoj uredbi o zaštiti podataka (pravo na dobivanje informacija o obradi njihovih osobnih podataka, pravo na podnošenje zahtjeva za ispravak ili brisanje nepotpunih, netočnih ili zastarjelih osobnih podataka, zahtjev za ostvarivanje prava na brisanje osobnih podataka čija je svrha obrade već prestala ili koji su obrađeni bez odobrenja).

Također, u navedenim *Općim uvjetima poslovanja - X* spominje se i privola za prikupljanje osobnih podataka korisnika usluga Hotela, a koji se prema navodima iz Općih uvjeta poslovanja prikupljaju temeljem Pravilnika sustavu e-Visitor.

Isto tako, na izričit upit od strane službenika Agencije (tijekom provođenja nadzornih aktivnosti) iz kojih razloga nije i sadržana informacija/obavijest o prikupljanju podatak o CVC broju i preslikama identifikacijskih dokumenta, službenik za zaštitu podataka Hotela navodi kako se obrazac ne odnosi na rezervacije putem e-pošte te kako osobe koje rezerviraju Hotel putem e-pošte zaprimaju obrazac *Privole* koji sadrži podatak o obradi osobnih podataka, a koji se isto tako daje svakom gostu kada fizički dođe u Hotel.

Slijedom navedenog, a uzimajući u obzir odredbe članka 13. stavka 1. i 2. Opće uredbe o zaštiti podataka, kojim je definirano pravo ispitanika na dobivanje informacija o obradi njihovih osobnih podataka, ističemo kako je utvrđeno da predmetno društvo nije na odgovarajući način informiralo/pružilo obavijest o obradi osobnih podataka ispitanicima koji su rezervirali smještajnu jedinicu Hotela, a posebice informaciju o prikupljanju podataka o CVC broju sadržan na preslici bankovne kartice, a tako i osobnog dokumenta.

Predmetno društvo je u *Općim uvjetima poslovanja - X* dostupnim na internetskim stranicama nedovoljnom opsegu pojasnilo svrhu i pravnu osnovu obrade osobnih podataka ispitanika prilikom korištenja usluga Hotela. Dakle, ističemo kako je predmetno društvo moralo biti svjesno kako je Opća uredba o zaštiti podataka usmjerena na pojedinca i na zaštitu njegovih osobnih podataka. Stoga, predmetno društvo je bilo dužno informirati ispitanika koje vrste osobnih podataka u koju svrhu prikuplja, pravnu osnovu obrade osobnih podataka, na koji način se koriste osobni podaci, odnosno tko koristi osobne podatke te koje mjere zaštite osobnih podataka su poduzete. Također, poštujući načelo transparentnosti predmetno društvo je bilo dužno ispitaniku pružiti sve informacije o obradi njegovih osobnih podataka u sažetom, razumljivom i lako dostupnom obliku, upotrebom jasnog i jednostavnog jezika te ga je bilo dužno upoznati sa svim njegovim pravima koja mu pripadaju sukladno Općoj uredbi o zaštiti podataka.

Imajući u vidu obveze koje nalaže Opća uredba o zaštiti podataka voditeljima obrade, navodimo kako predmetno društvo nije na adekvatan način pružilo informacije ispitanicima o obradi njihovih osobnih podataka, koja uključuje i prikupljanje podataka o CVC broju i preslikama osobnih dokumenta kako to nalaže članka 13. Opće uredbe o zaštiti podataka. Isto tako, utvrđeno je kako predmetno društvo nije ispitanicima, čije osobne podatke prikuplja, priopćilo sve potrebne informacije/obavijesti koje se smatraju nužnima za poštenu i transparentnu obradu osobnih podataka.

Nadalje, vezano uz obrazac *Privole* koji se ispitanicima dostavlja u trenutku rezervacije smještajne jedinice Hotela putem elektroničke pošte, a u kojem predmetno društvo na nedovoljno jasan način pruža informacije o obradi osobnih podataka ispitanicima čije podatke prikuplja, s tim u vezi ističemo, da predmetno društvo ne razlikuje privolu (kao jednu od mogućih pravnih osnova) od pružanja informacija/obavijesti ispitaniku o obradi njegovih osobnih podataka sukladno članku 13. Opće uredbe o zaštiti podataka.

U konkretnom slučaju, između ostaloga, predmetno društvo putem obrasca *Privole* nije osobama na transparentan način pružilo informacije o obradi njihovih osobnih podataka, odnosno o razlogu zbog kojih predmetno društvo traži dostavu podataka o CVC broju te presliku/sken osobnog dokumenta.

Stoga, uzimajući u obzir odredbe propisa kojima je regulirana zaštita podataka, ova Agencija ne može prihvatiti gore navedene obrasce/dokumente kao valjane, odnosno iste smatrati usklađenima sa odredbama Opće uredbe o zaštiti podataka, posebice uzimajući u obzir da se iz postupanja predmetnog društva dade zaključiti kako isti jasno ne razlikuje privolu - kao pravnu osnovu i informaciju/obavijest o obradi osobnih podataka.

Upravo iz gore navedenog, s aspekta pravnog okvira zaštite osobnih podataka, navodimo kako u konkretnom slučaju predmetno društvo prilikom prikupljanja osobnih podataka ispitanika-osoba koje rezerviraju smještaj u Hotelu nije poštivalo odredbe članka 13. stavka 1. i 2. Opće uredbe o zaštiti podataka. Predmetno društvo nije ispitanicima pružilo konkretne, jasne i nedvosmislene informacije o obradi njihovih osobnih podataka, također uz navođenje jasne svrhe obrade osobnih podataka i pravne osnove.

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.

Slijedom navedenog, voditelj obrade, u ovom slučaju društvo X ima obvezu uspostaviti mjere za učinkovitu primjenu načela zaštite podataka i provedbu zaštitnih mjera u obradi osobnih podataka, a sve kako bi osobni podaci ispitanika bili na odgovarajući način zaštićeni. Osim navedenog, predmetno društvo je dužno provoditi odgovarajuće organizacijske mjere zaštite osobnih podataka na način da internim aktima društva (primjerice: pravilnik o zaštiti osobnih podataka, pravilnik o informacijskoj sigurnosti) regulira/uredi područje zaštite osobnih podataka, odnosno uredi cjelokupni proces obrade osobnih podataka vezan uz pružanje usluga Hotela, a tiče se ostvarivanja sigurnosti obrađivanih osobnih podataka. Također predmetno društvo dužno je ovlastiti osobe za pristup osobnim podacima na način da osigura da svaki zaposlenik prilikom pristupa računalnim programima i e- pošti koristi svoje personalizirano korisničko ime i lozinku, a sve kako bi se znalo u kojem trenutku je netko imao pristup osobnim podacima (evidenciji osobnih podataka), a čime bi se spriječilo mogući neovlašteni pristup osobnim podacima. Isto tako, kada govorimo o ovlaštenju pristupa osobnim podacima, predmetno društvo dužno je odrediti koja radna mjesta, sukladno poslovnim procesima, imaju pravo pristupa i u kojem opsegu osobnim podacima koji su sadržani u evidencijama/bazama predmetnog društva, a koji su nužni za obavljanje njihovog posla.

Također, predmetno društvo dužno je kontinuirano podizati svijest o važnosti zaštite osobnih podataka svojih zaposlenika na način da isti budu svjesni koje sve osobne podatke koriste i obrađuju u svom svakodnevnom radu, kojim kategorijama osobnih podataka ti podaci pripadaju, gdje se ti podaci nalaze, koji su potencijalni rizici od krađe, zlouporabe i gubitka tih podataka, na koji način te podatke mogu zaštititi, kako se to negativno može reflektirati na poslovni subjekt u kojem rade, a u krajnjoj mjeri i na njih same, da je potrebno svakodnevno se pridržavati preporučenih i propisanih mjera zaštite radi smanjenja potencijalnih rizika od neovlaštenog pristupa i zlouporabe na najmanju moguću mjeru.

U konkretnom slučaju, društvo X dužno je procijeniti mogući rizik za osobne podatke ispitanika kada su isti slani putem e-pošte. Stoga je predmetno društvo je bilo dužno upozoriti ispitanika o potencijalnim rizicima vezanim uz uporabu e-pošte i o mogućnosti poduzimanja mjera zaštite osobnih podataka sadržanih u dokumentima koje isti šalju na e-mail adresu Hotela kao npr. informirati ispitanike putem svoje web stranice kako zaštititi email korespondenciju uporabom PGP enkripcije koja uključuje privatne i javne ključeve ili ih informirati na mogućnost zaključavanja dokumenata i slanja istom društvu lozinke za otključavanje drugim kanalima komunikacije kao što je npr. putem mobilnog telefona.

Temeljem gore navedenog, u provedenom upravnom postupku, utvrđeno je kako društvo X nije na adekvatan način provelo tehničke i organizacijske mjere zaštite osobnih podataka i na taj način povrijedilo je odredbe članka 32. stavka 1. a) i d) i članka 32. stavka 4. Opće uredbe o zaštiti podataka.

Nadalje, tijekom provođenja nadzornih aktivnosti utvrđeno je da je predmetno društvo službenika za zaštitu podataka imenovalo Y iz ____ koji je ujedno i imenovani voditelj Hotela.

S tim u vezi, navodimo kako odredbe članka 38. stavka 6. propisuju da službenik za zaštitu podataka može ispunjavati i druge zadaće i dužnosti. Voditelj obrade ili izvršitelj obrade osigurava da takve zadaće i dužnosti ne dovedu do sukoba interesa.

Slijedom navedenog, predmetno društvo je prilikom imenovanja službenika za zaštitu podataka moralo biti svjesno da postoji sukob interesa u odnosu na zadaće i dužnosti koje isti obavlja. Dakle, iz samog opisa poslova koje je ovoj Agenciji dostavilo predmetno društvo razvidno je kako je isti obavljao poslove u svojstvu voditelja Hotela koji su zahtijevali sustavno praćenje osobnih podataka i donošenja ključnih odluka vezanih za obradu osobnih podataka. Iz samog opisa poslova voditelja Hotela proizlazi da je isti velikom mjerom odgovoran za donošenje nekih upravljačkih odluka na razini obrade osobnih podataka, a dok je s druge strane kao službenik za zaštitu podataka dužan pratiti usklađenost poslovanja predmetnog društva u obradi osobnih podataka sa propisima kojima je regulirana zaštita osobnih podataka.

Stoga utvrđeno je kako se predmetno društvo nije rukovodilo odredbama članka 38. stavka 6. Opće uredbe o zaštiti podataka kada je istoga imenovalo službenikom za zaštitu podataka te je i tom dijelu utvrđeno kršenje.

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 izrekla 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 i glede iste izrečena upravna novčana kazna 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 podatka o CVC broju (sigurnosni kontrolni broj bankovne kartice) te preslike osobnih dokumenata, a tako i glede pružanja adekvatnih informacija/obavijesti ispitanicima o obradi njihovih osobnih podataka u konkretnu svrhu (primjerice rezervacija smještaja Hotela). Time se treba 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 15 000 000 EUR, ili u slučaju poduzetnika do 4 % ukupnog godišnjeg prometa na svjetskoj razini za prethodnu financijsku godinu, ovisno o tome što je veće.

Uvidom u sudski registar utvrđeno je da godišnji promet u 2022. godini za društvo X iznosi 9.473.128,00 kuna, odnosno 1.257.300,15 EUR, 4% tog iznosa je 50.292,006 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., članka 13. stavak 1. i 2., članka 32. stavka 1. točke a) i d) i stavka 4. i članka 38. stavka 6. Opće uredbe o zaštiti osobnih podataka izrekla voditelju obrade društvu X upravnu novčanu kaznu u iznosu od 15.000,00 EUR, a koji iznos čini 0,075 % u odnosu na maksimalni iznos upravne novčane kazne koju je u konkretnom slučaju Agencija mogla, odnosno bila ovlaštena izreći.

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 travnja 2019. godine bez pravne osnove obrađivao podatak o CVC broju uz dostavu preslike osobnog dokumenta sa fotografijom (osobna iskaznica, putovnica, vozačka dozvola), a sve iz razloga da se može teretiti kreditna kartica ispitanika koji je zatražio rezervaciju smještajne jedinice Hotela. Također, utvrđeno je kako društvo X nije poduzeo odgovarajuće organizacijske i tehničke mjere zaštite kod obrade osobnih podataka ispitanika čime je došlo do povrede članka 32. stavka 1. a) i d) i članka 32. stavka 4. Opće uredbe o zaštiti podataka.

Isto tako, voditelj obrade o predmetnoj obradi nije informirao ispitanike sukladno načelu transparentnosti pa su na taj način ispitanici bili zakinuti za osnovne informacije o obradi podataka, a sve sukladno članku 13. Opće uredbe o zaštiti podataka.

Uzimajući u obzir da je kod rezervacije smještaja u Hotelu predmetno društvo od ispitanika prikupljalo veći opseg osobnih podataka koji su sadržani na preslikama osobnih dokumenata, a koja je podrazumijevala i prikupljanje većeg opsega podataka koji nije nužan u odnosu na svrhu pružanja rezervacije smještaja, Agencija je prethodne okolnosti kvalificirala kao teže kršenje odredaba Opće uredbe o zaštiti podataka.

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

U odnosu na navedeno, 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);

Društvo X snosi odgovornost iz razloga što nije poduzelo dodatne odgovarajuće radnje kako bi svoje poslovanje, koje između ostalog obuhvaća i obradu osobnih podataka ispitanika, uskladilo sa odredbama Opće uredbe o zaštiti podataka. Isto tako, predmetno društvo nije poduzelo odgovarajuće tehničke i organizacijske mjere zaštite osobnih podataka koje bi omogućile određeni stupanj sigurnosti obrade osobnih podataka. Kao otegotna okolnost uzeta je obzir činjenica kako je predmetno društvo obrađivalo osobne podatke u prekomjernom opsegu uključivo CVC broj ispitanika (kontrolni broj bankovne kartice), a tako i tražilo dostavu presliku osobnog dokumenta ne vodeći računa da svi ti osobni podaci sa osobnog dokumenta nisu nužni za konkretnu svrhu obrade- rezervacije smještajne jedinice. Takvim nemarnim postupanjem predmetnog društva postojao je veliki rizik za zlouporabu osobnih podataka ispitanika.
- 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);

X je tijekom ovog upravnog postupka na odgovarajući način odgovaralo na zahtjeve nadzornog tijela.

- 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 tako osobni dokumenti, sadrže veliki opseg osobnih podataka čije prikupljanje u konkretnom slučaju nije bilo nužno za ostvarivanje svrhe zbog kojih se isti prikupljaju/ traže od ispitanika. Gore navedeno 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 sukladno članku 42. Zakona o općem upravnom postupku.

- 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);

X u vezi s istim predmetom nije prethodno izrečena mjera iz članka 58. stavka 2. Opće uredbe o zaštiti podataka.

- 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 primjenjivo u predmetnom slučaju.

- 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. Dakle, radi se o voditelju obrade čije poslovanje se sastoji od obrade osobnih podataka ispitanika te je takvim postupanjem došlo do prikupljanja osobnih podataka bez postojanja odgovarajuće pravne osnove, a isto tako su prikupljani osobni podaci koji nisu nužni za svrhe u koju su se isti prikupljali (svrha rezervacije smještajnog objekta).

Dakle, takvim postupanjem predmetnog društva dade se zaključiti kako isto nije bilo u dovoljnoj mjeri svjesno da za prikupljanje osobnih podataka (između ostalog i financijskih podataka) mora postojati odgovarajuća pravna osnova uz pružanje prethodne transparentne obavijesti/informacije ispitaniku o obradi njegovih osobnih podataka.

Agencija smatra da će izricanje iste dovesti do toga da voditelj obrade pravovremeno i odgovarajuće ispunjava svoje obveze u području zaštite osobnih podataka u budućnosti, a osobito u pogledu implementiranja odgovarajućih tehničkih i organizacijskih mjera koje omogućavaju učinkovitu primjenu načela zaštite podataka, a tako i postojanja svijesti o nužnosti prikupljanja osobnih podataka ispitanika i postojanju pravne osnove za takvo prikupljanje.

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 je iznos izrečene novčane kazne razmjeran povredi, pri čemu se posebno vodilo računa o težini povrede te financijskom poslovanju voditelja obrade koji je počinio povredu.

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 utvrdila činjenično stanje te je na temelju utvrđenog činjeničnog stanja pravilno primijenila materijalno pravo i izvela pravilan zaključak o činjeničnom stanju u konkretnom predmetu. Svoju odluku temelji na svim relevantnim dokazima i činjenicama kojima je raspolagala 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. X
2. Pismohrana, ovdje