



**REPUBLIKA HRVATSKA
AGENCIJA ZA ZAŠTITU
OSOBNIH PODATAKA**

KLASA: UP/I-034-01/21-01/03

URBROJ: 567-12/07-22-01

Zagreb, 24. siječnja 2022.

Agencija za zaštitu osobnih podataka na temelju članka 57. stavka 1., članka 58. stavka 1. i 2. točke (i) i članka 83. stavka 2. i 4. 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. i 45. 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) po službenoj dužnosti donosi sljedeće

RJEŠENJE

1. Utvrđuje se da je nepoduzimanjem odgovarajućih mjera sigurnosti obrade osobnih podataka od strane društva Konzum Plus d.o.o. iz Zagreba, Ulica Marijana Čavića 1/a, kao voditelja obrade, protivno članku 32. stavku 1. točke b) i d) te stavku 2. i 4. Opće uredbe o zaštiti podataka, došlo do neovlaštene obrade osobnih podataka ispitanika njihovom javnom objavom na društvenim mrežama i u medijima.
2. Za kršenje opisano u točki 1. izreke ovog rješenja, u skladu s odredbama članka 83. stavka 2. i 4. točke a) Opće uredbe o zaštiti podataka, izriče se društvu Konzum Plus d.o.o. iz Zagreba, Ulica Marijana Čavića 1/a, upravna novčana kazna u iznosu od:

675.000,00 kuna

(slovima: šestosedamdesetpetisuća kuna)

Društvo Konzum Plus d.o.o. iz Zagreba, Ulica Marijana Čavića 1/a 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: 6092-25860-340121013 s naznakom – "upravne novčane kazne koje izriče AZOP".

3. Ukoliko društvo Konzum Plus d.o.o. iz Zagreba, Ulica Marijana Čavića 1/a, u roku od 15 dana od pravomoćnosti ovog rješenja ne plati izrečenu upravnu novčanu kaznu, Agencija 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.
4. Društvo Konzum Plus d.o.o. iz Zagreba, Ulica Marijana Čavića 1/a, je dužno u roku od 15 dana od izvršene uplate dostaviti dokaz o uplati na uvid ovoj Agenciji.

O b r a z l o ž e n j e

I. UTVRĐENJE POVREDE

Agenciji za zaštitu osobnih podataka (dalje u tekstu: Agencija) obratio se voditelj obrade Konzum Plus d.o.o. iz Zagreba, Ulica Marijana Čavića 1/a, 10000 Zagreb, dana 04. prosinca 2020. godine sukladno članku 33. stavku 1. Opće Uredbe o zaštiti podataka s Izvješćem o povredi osobnih podataka ispitanika u kojem navodi da su radnici Konzum plus d.o.o. neovlašteno i protivno internim aktima i uputama Konzuma mobitelom snimili snimku video nadzora koja prikazuje fizički obračun dvoje kupaca, da je o predmetnoj snimci dana 30.11.2020. godine obaviješten Sektor marketinga Konzuma i to od strane novinara, da je u svrhu utvrđivanja radi li se o povredi osobnih podataka ispitanika Konzuma, provedena interna kontrola 02.12.2020. godine kojom je utvrđeno da je sporna snimka nastala 21.05.2020. godine u Konzum prodavaonici na adresi: trg A. Starčevića 10, Osijek, da je neovlaštenu snimku snimio radnik Konzuma i to na temelju naloga voditeljice dućana, te da je snimka neovlašteno distribuirana putem WhatsApp mobilne aplikacije za dopisivanje a navode da nije utvrđeno tko je snimku distribuirao na navedeni način. Isto se navodi da je vrijeme saznanja o predmetnoj povredi 02.12.2020. godine u 08:17 sati.

U svrhu utvrđenja točnog i potpunog činjeničnog stanja vezanog uz predmetnu povredu osobnih podataka Agencija je dopisom KLASA:042-03/20-01/143, URBROJ:567-12/07-20-02 od 15. prosinca 2020., a u skladu sa svojim ovlastima, zatražila od voditelja obrade Konzum plus d.o.o. dostavu preslike akata voditelja obrade Konzum plus d.o.o. odnosnih na uređenje obrade osobnih podataka unutar istog, podatak i relevantnu dokumentaciju glede sigurnosti obrade osobnih podataka, odnosno tehničkih i organizacijskih mjera koje provodi predmetni voditelj obrade, posebice vezane uz videonadzorni sustav, također, u odnosu na videonadzorni sustav postavljen u trgovini na adresi Trg A. Starčevića 10, Osijek, dostavu relevantnih informacija odnosnih na sigurnost obrade osobnih podataka, odnosno tehničkih i organizacijskih mjera koje provodi predmetni voditelj obrade.

Dodatno je zatražena dostava informacija i relevantne dokumentacije što je Konzum plus d.o.o. sve utvrdio te što je poduzeo vezano i nastavno na predmetni incident u smislu organizacijskih i tehničkih mjera odnosnih na sigurnost obrade osobnih podataka putem videonadzornog sustava.

U odnosu na zatraženo, Agencija je dana 24. prosinca 2020. godine zaprimila od strane društva Konzum plus d.o.o. pisano očitovanje od 23. prosinca 2020. godine, kojim se dostavljaju, kako navode, interni akti odnosni na zaštitu osobnih podataka, implementirani prije navedenog incidenta a u okviru postupka usklađenja poslovanja Konzuma s Općom uredbom o zaštiti podataka, te informacije vezane uz predmetnu povredu i to; preslika *Pravilnika o zaštiti osobnih podataka v 2.0.* od 10.07.2018., preslika akta *Uloge i odgovornosti za zaštitu osobnih podataka v 1.0.* od 20.07.2018., preslika akta *Proces i metodologija procjena učinka na privatnost v 2.0.* od 16.07.2018., Preslika akta „*Privacy by design*“ i „*Privacy by Default*“ od 23.07.2018., preslika *Plana upravljanja izvješćivanja o sigurnosnim incidentima v 1.0.* od 13.08.2018., *Sigurnosni plan zaštite tvrtke Konzum plus d.o.o.* od 15.02.2019., preslika *Sigurnosne procedure-KONZUM P-0915, Osijek, Trg. A. Starčevića 10* od 19.11.2015., preslika *Uputa za prodavaonice* od 03.09.2019., preslika *Edukativnog materijala za prodavaonice – Mjere zaštite i sigurnosti* od lipnja 2017., fotografije zaslona nadzornog monitora koji se nalazi u uredu voditeljice prodavaonice iz kojih je razvidan zahvat kamera koje snimaju blagajne, prodajni prostor, sef, vanjske ulaze i skladište u prodavaonici, fotografije postave kamera, fotografije obavijesti o postavljenom videonadzornom sustavu, fotografije zaslona nadzornog monitora iz kojih su razvidne dostupne snimke, a sve odnosne na prodavaonicu Konzum plus d.o.o. na adresi Trg Ante Starčevića 10, Osijek, preslika *Ugovora broj _____ o pružanju usluga redovnog i izvanrednog održavanja sustava tehničke zaštite* od 19.07.2019., preslika *Ugovora broj _____ o pružanju usluga ugradnje/nadogradnje sustava tehničke zaštite na objektima naručitelja* od 19.07.2019., preslika *Ugovora o obradi podataka* između Konzum plus d.o.o. kao voditelja obrade i Sokol d.o.o. kao izvršitelja obrade od 05.07.2019., preslika *Izješća korporativne sigurnosti o neprimjerenom video isječku*, preslike *Upozorenja na mogućnost otkaza Ugovora o radu* od 07.12.2020., preslike *Izjave _____, _____, _____*, preslika *GDPR – Edukacija za dućane*, preslika *Pitanja provjere znanja*, preslika *Uvjerjenja o provedenoj edukaciji za gđu. _____ i _____*, preslika *Izjave o povjerljivosti osobnih podataka i obradi osobnih podataka radnika _____, _____*, preslika *Pravilnika o zaštiti osobnih podataka v 2.0* od 11.12.2020., preslika evidencije obrade osobnih podataka za video nadzor, preslika analize legitimnog interesa za video nadzor, preslika analize rizika video nadzora.

Uvidom u *Izješće korporativne sigurnosti društva Konzum plus d.o.o.* o neprimjerenom video isječku navodi se: „Dana 30. studenog 2020. godine došli smo do saznanja da se putem društvenih mreža distribuira kratki video isječak vezan uz konfliktnu situaciju u jednom od Konzumovih prodajnih mjesta. Iz uvida u video isječak vidljivo je da isti traje 50 sekundi, a sadržajno se radi o verbalnom fizičkom obračunu dvojice nepoznatih muških osoba starije životne dobi (55-60 godina), do kojeg je došlo na naplatnom mjestu u jednom od prodajnih mjesta Konzum plus d.o.o. U pozadini je zabilježen tonski zapis komentara nekoliko osoba, koji funkcionalno ne pripada originalnom video zapisu. Tijekom provedene istrage došli smo do saznanja da je predmetna video snimka originalna, te da je izvorno nastala na način da je putem mobitela sniman ekran službenog video nadzora Konzuma, dana 21.05.2020. god. oko 11.00 sati na prodajnom mjestu Trg A. Starčevića 10, Osijek, da je utvrđen identitet osoba koje

su snimale službeni video nadzor, tj. osobe koje su komentirale cijeli događaj, a to su
Snimku je na svoj mobitel po uputi
snimio isti je snimljeni sadržaj prosljedio gđi.
koja prosljeđuje snimku direktoru regije . Nakon što je
istu pregledao je naložio da se snimka izbriše i ne distribuirati drugim osobama. Zbog
proteka vremenskog perioda od pet mjeseci, nismo uspjeli utvrditi tko i na koji je način ovu
snimku distribuirao u javnost prema društvenim mrežama i medijima. “.

Uvidom u sadržaj Ugovora broj o pružanju usluga redovnog i izvanrednog
održavanja sustava tehničke zaštite od 19.07.2019. i Ugovora broj o pružanju
usluga ugradnje/nadogradnje sustava tehničke zaštite na objektima naručitelja od 19.07.2019.,
sklopljenih između voditelja obrade Konzum plus d.o.o. i izvršitelja obrade Sokol d.o.o.
utvrđeno je da je predmetni videonadzorni sustav u poslovnicu P-0915 Konzum plus d.o.o. na
adresi Trg A.Starčevića 10, Osijek, postavilo i održava društvo Sokol d.o.o. iz Zagreba, Trg
Republike Hrvatske 8/II.

Uvidom u sadržaj Ugovora o obradi podataka od 05.07.2019. između Konzum plus d.o.o. kao
voditelja obrade i Sokol d.o.o. kao izvršitelja obrade, članak 1. navodi: “Izvršitelj je upoznat
kako mu upute u ime Voditelja, a glede obrade osobnih podataka, mogu davati isključivo osobe
naveden u Prilogu br. 2 Ugovora“, članak 7. navodi: „Izvršitelj će uspostaviti svoju internu
organizaciju na način kojim ispunjava posebne zahtjeve za zaštitu podataka, kako i poduzeti
tehničke i organizacijske mjere za primjerenu zaštitu podataka, posebice vodeći računa o
zahtjevima iz čl. 32 Uredbe, Izvršitelj će obavijestiti Voditelja o novim tehnologijama s kojima
se upozna i pomoću kojih se zaštita obrade podataka može podići na višu (sigurniju ili
praktičniju) razinu - u tom smislu, u prva tri mjeseca svake kalendarske godine, Izvršitelj će
poslati pisano očitovanje Voditelju o svojim prijedlozima po ovom pitanju (ili očitovanje kako
ih nema), Izvršitelj će primjenjivati pseudonimizaciju (kao obveznu sigurnosnu mjeru tzv.
privacy by default) i enkripciju osobnih podataka u mjeri u kojoj je to razumno moguće kako
bi se osigurala primjena razine sigurnosti, Izvršitelj će predložiti sigurnosno prihvatljiv način
razmjene osobnih podataka s Voditeljem“, Prilog 3, Tehničke i organizacijske mjere, poglavlje
1. Povjerljivost, Video nadzor, točka 1.1. navodi: “Izvršitelj mora voditi pregled pristupa
sustavu video nadzora kod Voditelja, tako da je jasno koji zaštitar je u koje doba imao pravo
pristupa. Ako se pregledavaju snimke video nadzora, zaštitar mora naznačiti u koju svrhu se
vrši pregled te po čijem nalogu. Mediji za evidenciju omogućuje Voditelj.“, a u poglavlju 2.
Integritet, Video nadzor, točka 2.1. navodi: „Prijenos podataka radi se putem USB sticka gdje
se dokument odnosno pristup istima štiti s dodatnom lozinkom. Lozinka se predaje Konzumu
zasebnim putem osobi navedenoj u Prilogu br. 2 ovog Ugovora, na siguran način, primjerice
enkriptiranim e-mailom ili servisima koji koriste end-to-end enkripciju (npr. WhatsApp, Viber,
Signal). “

Uvidom u sadržaj Pravilnika o zaštiti osobnih podataka Konzum d.d. v 2.0. od 10.07.2018.,
poglavlje XI., Sigurnost i zaštita osobnih podataka navodi se: “Konzum je dužan
implementirati te kontinuirano održavati i nadzirati tehničke i organizacijske mjere koje za cilj
imaju osiguravanje povjerljivosti, integriteta i raspoloživosti osobnih podataka. Sukladno

tome, Konzum će implementirati procese koji će osigurati da niti jedan sustav koji obrađuje osobne podatke nije pušten u produkcijski rad bez da je ispunio propisane standarde sigurnosti zaštite. S ciljem kvalitetnog i odgovornog upravljanja aspektima zaštite osobnih podataka iz perspektive informacijske sigurnosti, Konzum je uspostavio funkciju Voditelja sigurnosti informacijskog sustava s jasno definiranim ulogama i odgovornostima. Mjere za osiguravanje povjerljivosti, integriteta i raspoloživosti osobnih podataka biti će bazirane na konceptu procjene rizika. Procjene rizika provodit će se periodički na svim sustavima koji obrađuju osobne podatke te će sukladno nalazima biti implementirane odgovarajuće sigurnosne mjere. Svi sigurnosni rizici koji nisu adekvatno tretirani moraju biti prihvaćeni od strane Uprave, a Službenik za zaštitu osobnih podataka mora biti s njima pravovremeno upoznat. Pritom prepoznate su određene sigurnosne kontrole kao ključne za zaštitu osobnih podataka i koje kao takve moraju biti ispravno implementirane na svim sustavima koji obrađuju osobne podatke: detaljno bilježenje log zapisa i sigurnosnih događaja, prosljeđivanje log zapisa na središnji sustav za upravljanje log zapisima, centralizirano upravljanje pravima pristupa i privilegijama, dodjela prava pristupa u skladu s načelima minimalnih privilegija i poslovnom potrebom“.

Uvidom u sadržaj Pravilnika o zaštiti osobnih podataka Konzum plus d.o.o. v 0.2 od 11.12.2020. poglavlje XVI. Sigurnost i zaštita osobnih podataka, utvrđeno je da je sadržajno proširen u odnosu na prethodno citirani Pravilnik od 10.07.2018. (poglavlje XI.) dijelom: “Radnicima je zabranjeno svako neovlašteno i nepotrebno umnožavanje, kopiranje, spremanje i/ili prenošenje osobnih podataka ispitanika. Svu dokumentaciju koja sadrži osobne podatke, kako i podatke koji su sadržani u informatičkim sustavima Konzuma, radnici su obvezni čuvati kao povjerljive. Radnici su obvezni voditi računa da se sva fizička dokumentacija koja sadrži osobne podatke (ugovori u kojima su navedeni kontakt podaci fizičkih osoba – ispitanika, dokumentacija o radnicima i druga dokumentacija koja sadrži osobne podatke ispitanika) čuva i pohranjuje uz primjenu svih odgovarajućih i razumnih mjera kojima se osigurava njezino odgovarajuće čuvanje, uključujući pritom mjere zaštite od oštećenja, uništenja i gubitka. Radnici se obvezuju da će sukladno važećim promjenjivim propisima čuvati povjerljivost svih osobnih podataka kojima imaju pravo i ovlasti pristupa, a koji se nalaze u registru (evidenciji) osobnih podataka koje vodi Konzum te da će iste osobne podatke koristiti isključivo i samo u točno određenu (propisanu) svrhu, sukladno nalogima i uputama Konzuma te u okviru poslova definiranih ugovorom o radu i promjenjivim internim aktima Konzuma. Radnici su dužni poštovati privatnosti i povjerljivost osobnih podataka ispitanika te postupati u skladu s organizacijskim i tehničkim mjerama predviđenim za njihovu zaštitu. Radnici ne smiju osobne podatke ispitanika dostavljati/davati na korištenje niti na bilo koji drugi način učiniti dostupnim trećim (neovlaštenim) osobama te se obvezuju da će povjerljivost istih osobnih podataka čuvati i nakon prestanka ovlasti pristupa osobnim podacima odnosno po prestanku radnog odnosa iz bilo kojeg razloga. Radnicima je zabranjeno saznanja i podatke o osobnim podacima ispitanika dalje prikupljati, obrađivati, objavljivati i/ili prenositi na bilo koji način. U slučaju zahtjeva Konzuma ili nadležnih tijela u skladu s odredbama primjenjivih propisa te u slučajevima definiranim u istim, radnik je obavezan uništiti papirnati i elektronski zapis navedenih osobnih podataka kao i sve postojeće kopije.“.

Uvidom u Sigurnosni plan zaštite tvrtke Konzum plus d.o.o. od 15.02.2019. poglavlje IX. ZAŠTITA PODATAKA, članak 39. Video nadzor, navodi se: "Obrada osobnih podataka putem video nadzora može se provoditi samo u svrhu koja je nužna i opravdana za zaštitu osoba i imovine. Voditelj obrade podataka je tvrtka Konzum plus d.o.o.. Zahtjev za izradu snimke/fiksiranje video zapisa kreira se putem elektronskog OTRS naloga. Fiksiranje video zapisa dozvoljeno je isključivo od strane ovlaštenih djelatnika ugovornog zaštitarskog društva i djelatnika Službe korporativne sigurnosti. Sve snimke video nadzora fiksirane na CD ili drugi medij dostavljaju se i arhiviraju u sjedištu Tvrtke, te se čuvaju sukladno mjerama navedenim u članku 37. ovog Dokumenta. Snimanje kadrova video nadzora na mobilne telefone i druge slične uređaje nije dozvoljeno. Za pristup pregledu i snimkama video nadzora uspostavlja se sustav logova za evidentiranje pristupa snimkama video nadzora (vrijeme i mjesto pristupa, osoba koje je izvršila pristup snimkama). U navedenu svrhu kreiraju se lozinke za pristup snimačima kako je niže navedeno: Voditelj obrade – sve ovlasti, zamjenik voditelja obrade-sve ovlasti, izvršitelj obrade 1 - ovlasti gledanja uživo, pregledavanje zapisa, fiksiranje video zapisa, izvršitelj obrade 2 – ovlast gledanja uživo i pregledavanje zapisa, serviser – sve ovlasti osim pregleda logova, zaštitar – ovlast gledanja uživo i pregledavanja zapisa, a članak 40. Kontrola pristupa navodi: "Svrha sustava kontrole pristupa je da onemogući ulaske neovlaštenim osobama uštićene prostore, te da omogući ulazak onih osoba koje za ulazak imaju odobrenje. Sustavi kontrole pristupa svih poslovnih prostora upravnih zgrada povezani su na centralni server koji sadrži bazu podataka i izvodi glavnu aplikaciju. Aplikacija komunicira s lokalnim kontrolerima koji na nivou pojedinih vrata dopuštaju/brane prolaskes karticom. Sva komunikacija sustava odvija se putem informatičke mreže. U slučaju pada mreže kontroleri rade u režimu lokalnog odlučivanja tj. odlučuju sa zadnjim stanjem koje je zapisano na kontroloru. ".

Uvidom u sadržaj Uputa za prodavaonice od 03.09.2019 pod točkom 3. Ovlaštene osobe za pregled snimki navodi se: "Za pregled snimki ovlašteni su: Radnici ugovornog zaštitarskog društva koji obavljaju usluge zaštite osoba i imovine za potrebe Tvrtke, a kojima su na rukovanje u svakodnevnom radu povjereni sustavi tehničke zaštite (alarmni sustav, sustav video nadzora i dr.), radnici Službe korporativne sigurnosti i dr. osobe po njihovom ovlaštenju, voditelj /poslovođa prodavaonice i dr. osobe po njegovom ovlaštenju na razini ustrojstvene jedinice, zamjenik voditelja/poslovođe prodavaonice. "

Uvidom u Edukativni materijal za prodavaonice – Mjere zaštite i sigurnost od lipnja 2017., točka 16. Odgovorne osobe, navodi se: Odgovorna osoba za provođenje mjera zaštite na razini prodavaonice (ustrojstvene jedinice) je voditelj/poslovođa prodavaonice. Ovlaštene osobe za upravljanje ugrađenim sustavima tehničke zaštite na razini prodavaonice (ustrojstvene jedinice) su: voditelj/poslovođa prodavaonice i dr. osobe po njegovom ovlaštenju na razini ustrojstvene jedinice, zamjenik voditelja/poslovođe prodavaonice, radnici ugovornog zaštitarskog društva koji obavljaju usluge zaštite osoba i imovine za potrebe Tvrtke, a kojima su na rukovanje u svakodnevnom radu povjereni sustavi tehničke zaštite (alarmni sustav, sustav video nadzora i dr.). "

Uvidom *Edukativni materijal GDPR - Edukacija za dućane*, (nedatiran), navodi se: *"Snimanje snimki/kadrova video nadzora na mobilne ili bilo koje druge uređaje nije dozvoljeno, kao niti njihova distribucija putem društvenih mreža WhatsApp, Viber li bilo koja druge komunikacijske platforme. Nije dozvoljeno neovlaštenim osobama omogućiti uvid u snimke video nadzora niti otkrivati lozinke za pristup sustavu."*

Agencija je dopisom KLASA: 042-03/20-01/143, URBROJ: 567-12/07-20-04, od 04. siječnja 2021. zatražila očitovanje od društva Sokol d.o.o., Trg Republike Hrvatske 8/II, 10000 Zagreb u svezi predmetne povrede osobnih podataka te je zatražila dostavu informacija i relevantne dokumentacije i to: kada je društvo Sokol d.o.o. saznalo tj. postalo svjesno sigurnosnog incidenta navedenog u izvješću od 04. prosinca 2020. (navesti datum), da li je društvo Sokol d.o.o. o predmetnom incidentu obaviješteno od strane društva Konzum plus d.o.o. ili iz vlastitih izvora/ drugih izvora, da li u trgovini Konzum plus d.o.o. na adresi Trg A. Starčevića 10, Osijek zaštitar/i društva Sokol d.o.o. provodi/e fizičku i tehničku zaštitu, te da li se navedene aktivnosti provode u radnom vremenu i/ili izvan radnog vremena trgovine, tko od zaposlenika društva Sokol d.o.o. ima pravo pristupa učinjenim video zapisima predmetnog videonadzornog sustava, pod kojim okolnostima, s kojim ovlastima i na koji način, navesti implementirane sigurnosne mjere od neovlaštenog pristupa prostoriji gdje je smješten nadzorni monitor i videosnimači predmetnog videonadzornog sustava, te informaciju tko je nadležan za nadzor provedbe istih.

Uvidom u zaprimljeno očitovanje društva Sokol d.o.o. od 14. siječnja 2021. isti između ostalog navode da su za predmetni događaj saznali 03.12.2020. iz medija preko internet stranice SiB, da na navedenoj lokaciji u vrijeme spornog događaja nisu imali angažirane neposredne izvršitelje poslova tjelesne zaštite, da se monitor i snimač video nadzora nalaze u uredu voditeljice Konzum plus d.o.o. na navedenoj lokaciji, da pristup sustavu video nadzora imaju djelatnici zaštite Sokol d.o.o. ali samo po zahtjevu vlasnika sustava za servisiranjem ili izdvajanjem snimke pojedinog događaja uz prethodnu specifikaciju dana, sata i vremenskog intervala za koji se traži izdvajanje pojedine snimke, da po pitanju konkretnog slučaja takav zahtjev nisu zaprimili niti je snimka skidana sa snimača prodavaonice od strane tehničke službe društva.

Agencija je dopisom KLASA: 042-03/20-01/143, URBROJ: 567-12/07-20-07, od 03. svibnja 2021. zatražila od Konzum plus d.o.o. dodatno očitovanje i dostavu relevantne dokumentacije i to: da li je nastavno na predmetnu povredu osobnih podataka/incident došlo do izmjene *Sigurnosnog plana zaštite tvrtke Konzum plus d.o.o. od 15.02.2019., Sigurnosne procedure - KONZUM P-0915, Osijek, Trg Ante Starčevića 10, od 19.11.2015., Upute za prodavaonice od 03.09.2019., i Edukacijskog materijala za prodavaonice - Mjere zaštite i sigurnosti od 2017.*, te ukoliko je, navesti koje su izmjene nastale (posebice da li su mjere iz članka 32. Opće Uredbe o zaštiti podataka dodane /izmijenjene), da li su i koje dodatne organizacijske i tehničke mjere primijenjene nastavno na Incident i jesu li iste izvršene/provedene, te iskazati Agenciji, ako nije iskazano u prethodno navedenim očitovanjima i priložima i ako nije naznačeno u traženju dodatnog očitovanja, i druge eventualno relevantne činjenice i okolnosti za konkretan slučaj i/ili aspekte zaštite osobnih podataka kod društva Konzum plus d.o.o.

U odnosu na zatraženo, Agencija je dana 13. svibnja 2021. godine zaprimila od strane društva Konzum plus d.o.o. pisano očitovanje od 12. svibnja 2021. godine, koje navodi da: *“predmetni interni akti nisu izmijenjeni, izuzev u odnosu na edukacijske materijale. Naime, imajući u vidu način nastupa predmetnog incidenta poduzete su dodatne aktivnosti sa svrhom provedbe edukacije radnika zaposlenih u maloprodaji, odnosno dućanima Konzuma. U skladu s navedenim, a nakon hitne edukacije provedene odmah po saznanju za predmetni incident tijekom koje su dodatno educirani radnici uključeni u incident, organizirana je i provedena edukacija i za sve ostale radnike zaposlene u maloprodaji. Predmetna edukacija nije obuhvatila samo radnike u dućanima koji su ujedno i ovlaštene osobe za pristup i pregled snimkama, već i za sve radnike u maloprodaji, uključujući i studente, te je kao takva obuhvatila edukaciju ukupno 7569 radnika u dućanima. U navedenu su svrhu edukacijski materijali, u odnosu na verziju dostavljenu u našem očitovanju od 23.12.2020. godine, dodatno prošireni u dijelu definiranja načina postupanja sa snimkama videonadzora, odnosno ponašanja u prostorima u kojima se videonadzor nalazi. Tako je u edukacijskom materijalu izričito navedeno da neovlaštenim osobama nije dozvoljeno omogućiti uvid u snimke videonadzora niti otkrivati lozinke za pristup sustavu (neovlaštene osobe su sve osobe koje nemaju pravo pregleda snimki videonadzora, uključujući, ali ne ograničeno na: druge radnike Konzuma, radnike društva s kojim Konzum surađuje (npr. Multiplus card d.o.o. dobavljači Konzuma itd) da je ekran videonadzora potrebno okrenuti na način da samo ovlaštene osobe imaju pogled na isti kao i da ako postoji potreba da drugi radnici, osim ovlaštenih osoba, ulaze u prostor u kojem se nalazi videonadzor, isto je moguće samo u pratnji ovlaštenih osoba.”*

Isti dalje navode da su: *“u sve prostorije svih dućana Konzuma u kojima se nalazi videonadzor, na ekrane istog postavljene naljepnice na kojima je istaknuta zabrana snimanja snimki/kadrova videonadzora na mobilne ili druge uređaje te informacija da je uvid u snimke videonadzora dozvoljen samo ovlaštenim osobama.”*

Također se navodi: *“da je u vremenskom periodu od očitovanja od 23.12.2020. pa do dana slanja očitovanja od 12.05.2021. Uprava Konzuma usvojila novi Pravilnik o zaštiti osobnih podataka, kojim su u točki XVI. – SIGURNOST I ZAŠTITA OSOBNIH PODATAKA, između ostalih mjera zaštite osobnih podataka propisane i obveze glede postupanja radnika s osobnim podacima ispitanika. Radnicima je tako zabranjeno svako neovlašteno i nepotrebno umnožavanje, kopiranje, spremanje i/ili prenošenje osobnih podataka ispitanika. Istom je točkom definirano da su radnici sve podatke koji su sadržani u informatičkim sustavim Konzuma, obvezni čuvati kao povjerljive, kao i da će osobne podatke koristiti isključivo i samo u točno određenu (propisanu) svrhu, sukladno nalogima i uputama Konzuma te u okviru poslova definiranih ugovorom o radu i primjenjivih internih akata Konzuma. Nadalje je definirana zabrana radnicima glede dostavljanja osobnih podataka ispitanika trećim (neovlaštenim) osobama te obveza da će povjerljivost istih osobnih podataka čuvati i nakon prestanka ovlasti pristupa osobnim podacima, odnosno po prestanku radnog odnosa iz bilo kojeg razloga.”* Očitovanju se prilaže preslika GDPR Edukacija za maloprodaju, preslika naljepnice i fotografija naljepnice na ekranu, preslika Pravilnika o zaštiti osobnih podataka od 08.02.2021. i preslika Pravilnika o upravljanju incidentima od 22.03.2021.

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 (SL EU L119), sukladno njenom članku 99. stavku 2.

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

Člankom 5. stavkom 1. Opće uredbe o zaštiti podataka propisano je da osobni podaci moraju biti zakonito, pošteno i transparentno obrađivani s obzirom na ispitanika (načelo zakonitosti, poštenosti i transparentnosti); prikupljeni u posebne, izričite i zakonite svrhe te se dalje ne smiju obrađivati na način koji nije u skladu s tim svrhama (načelo ograničavanja svrhe); primjereni, relevantni i ograničeni na ono što je nužno u odnosu na svrhe u koje se obrađuju (načelo smanjenja količine podataka); točni i prema potrebi ažurni (načelo točnosti); čuvani u obliku koji omogućuje identifikaciju ispitanika samo onoliko dugo koliko je potrebno u svrhe radi kojih se osobni podaci obrađuju (načelo ograničenja pohrane) i obrađivani na način kojim se osigurava odgovarajuća sigurnost osobnih podataka, uključujući zaštitu od neodgovarajuće ili nezakonite obrade te od slučajnog gubitka ili uništenja, primjenom odgovarajućih tehničkih ili organizacijskih mjera (načelo cjelovitosti i povjerljivosti).

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: (b) sposobnost osiguravanja trajne povjerljivosti, cjelovitosti, dostupnosti i otpornosti sustava i usluga obrade i (d) proces za redovno testiranje, ocjenjivanje i procjenjivanje učinkovitosti tehničkih i organizacijskih mjera za osiguravanje sigurnosti obrade, dok je stavkom 2. istoga članka propisano da se prilikom procjene odgovarajuće razine sigurnosti u obzir posebno uzimaju rizici koje predstavlja obrada, posebno rizici od slučajnog ili nezakonitog uništenja, gubitka, izmjene, neovlaštenog otkrivanja osobnih podataka ili neovlaštenog pristupa osobnim podacima koji su preneseni, pohranjeni ili na drugi način obrađivani, a stavkom 4. istoga članka je propisano da

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 obavezan učiniti prema pravu Unije ili pravu države članice.

U ovoj upravnoj stvari utvrđeno je da je dana 21.05.2020. oko 11 sati zaposlenik društva Konzum plus d.o.o., na prodajnom mjestu Trg A. Starčevića 10, Osijek, po uputi [redacted], voditeljice poslovnice na istoj adresi, uz prisustvo treće osobe, [redacted], mobitelom snimio monitor videonadzornog sustava poslovnice a na kojem je bio prikazan video zapis dvojice muškaraca starije životne dobi u fizičkom sukobu u trajanju od 50 sekundi. [redacted] je učinjenu snimku zatim mobitelom proslijedio koja je istu prosljedila direktoru regije [redacted]. Nakon što je istu pregledao [redacted] je naložio da se snimka izbriše i ne distribuira drugim osobama. Predmetni video zapis postao je dostupan na društvenim mrežama a zatim je objavljen i u medijima 03. prosinca 2020.

Vezano za navode voditelja obrade da se na spornoj video snimci prikazuju dvije muške osobe koje ulaze u fizički obračun od kojih je jedna većim dijelom snimke vidljiva samo s leđa, dok je drugi sudionik vidljiv na snimci i sprijeda, da je radnica Konzuma koja se nalazi na blagajni vidljiva iz profila, a radnica koja pokušava razdvojiti osobe u fizičkom konfliktu s leđa i sprijeda, da sama snimka nije povjerljiva jer je uzeta na području dućana označenom kao područje gdje se provodi snimanje, te da identitet snimanih osoba mogu utvrditi samo osobe koje osobno poznaju iste, Agencija ističe da su osobni podaci sukladno članku 4. stavku 1. točki 1. Opće uredbe o zaštiti podataka, svi podaci koji se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi. Sukladno uvodnoj izjavi 26. Opće uredbe o zaštiti podataka, kako bi se odredilo može li se identitet pojedinca utvrditi, trebalo bi uzeti u obzir sva sredstva, poput primjerice selekcije, koju voditelj obrade ili bilo koja druga osoba mogu po svemu sudeći upotrijebiti u svrhu izravnog ili neizravnog utvrđivanja identiteta pojedinca. Pri tome treba uzeti u obzir sve objektivne čimbenike, kao što su troškovi i vrijeme potrebno za utvrđivanje identiteta. Budući da je Agencija u ovoj upravnoj stvari utvrdila da se na predmetnom video zapisu mogu jasno razabrati crte lica, konstitucija, pokreti tijela te ostale fizičke značajke ispitanika, nedvojbeno je utvrđeno da se iz gore navedenih značajki mogu sa sigurnošću identificirati ispitanici/ sudionici predmetnog događaja. Dakle, Agencija je uzimajući u obzir sve navedeno, utvrdila da se u predmetnoj povredi radi o obradi osobnih podataka jer su snimkom obrađeni podaci koji se odnose na pojedinca čiji se identitet može izravno utvrditi.

Agencija je utvrdila da Konzum plus d.o.o. nije poduzeo adekvatne radnje kojima bi onemogućio svojem zaposleniku stvaranje snimke videonadzornog monitora koristeći mobilni uređaj. Naime, Konzum plus d.o.o. poduzeo je određene organizacijske mjere zaštite kao što su edukacije zaposlenika, usvajanje internih akata kojima se propisuje ovlaštenje pristupa učinjenim video zapisima, te potpisivanje izjave o povjerljivosti za zaposlenike, međutim iz spisa predmeta razvidno je da voditelj obrade nije poduzeo dovoljne, odnosno, odgovarajuće organizacijske i tehničke mjere sigurnosti, niti prije niti nakon incidenta/predmetne povrede osobnih podataka, a koje su mogle, odnosno trebale svesti rizik iste ili slične povrede na najmanju moguću razinu.

Također, razvidno je da voditelj obrade nije nadzirao provedbu tehničkih i organizacijskih mjera koje za cilj imaju osiguravanje povjerljivosti, integriteta i raspoloživosti osobnih podataka odnosno, propustio je redovno testirati, ocijeniti i utvrditi učinkovitost tehničkih i organizacijskih mjera predviđenih za osiguravanje sigurnosti obrade putem videonadzora.

Drugim riječima, nije dovoljno uspostaviti automatizirani sustav zapisa za evidentiranje pristupa snimkama videonadzora koji će sadržavati vrijeme i mjesto pristupa, kao i oznaku osoba koje su izvršile pristup podacima prikupljenim putem videonadzora, ukoliko se redovito ne provjerava postupaju li ovlaštene osobe sukladno internoj proceduri.

Naime, da je voditelj obrade redovito nadzirao provedbu tehničkih i organizacijskih mjera (primjerice kontrolom logova opravdanosti pristupa videonadzornom sustavu) takvim postupanjem bi isti bio u poziciji pravovremeno reagirati ukoliko se pokaže potreba uvesti dodatne tehničke i organizacijske mjere te iste pravodobno utvrditi i propisati.

Pri tom je potrebno uzeti u obzir da se u predmetnom slučaju radi o voditelju obrade koji je prema javno dostupnim informacijama vodeći trgovački lanac u Republici Hrvatskoj s više od 11.000 zaposlenika i preko 600 prodavaonica, prisutan u svim dijelovima Republike Hrvatske uključivo i većinu hrvatskih otoka, te je za očekivati da će isti zbog velikog broja ispitanika čiji se osobni podaci svakodnevno obrađuju putem video nadzornih sustava u njegovim prodavaonicama, kao i činjenice da veliki broj zaposlenika ima ovlaštenja pristupa učinjenim video zapisima, primijeni složenije mjere sigurnosti, nadzora i kontrole pristupa video zapisima.

Iz prethodno navedenih odredbi Opće uredbe o zaštiti podataka proizlazi da je voditelj obrade prilikom obrade osobnih podataka dužan poduzeti odgovarajuće tehničke mjere sigurnosti, na način da treba osigurati trajnu povjerljivost sustava kao i proces redovnog testiranja, ocjenjivanja i procjenjivanja učinkovitosti tehničkih i organizacijskih mjera za osiguravanje sigurnosti obrade, kao i poduzeti mjere kako bi osigurao da svaki pojedinac koji djeluje pod njegovom odgovornošću, a koji ima pristup osobnim podacima, ne obrađuje te osobne podatke ako to nije prema uputama voditelja obrade, a prilikom procjene odgovarajuće razine sigurnosti u obzir posebno uzeti rizike od, *inter alia*, neovlaštenog otkrivanja osobnih podataka. Nakon točno i potpuno utvrđenog činjeničnog stanja razvidno je da je izvršitelj obrade propustio provesti odgovarajuće mjere sigurnosti sukladno postojećim i predvidivim rizicima, čime je postupio protivno odredbi članka 32. stavka 1. točke b) i d) i stavka 2. i 4. Opće uredbe o zaštiti podataka.

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 voditelj 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 voditelj obrade.

Izricanjem upravne novčane kazne ujedno se želi postići da se poštuju pravila o zaštiti osobnih podataka kako od strane samog izvršitelja obrade tako i od svih drugih izvršitelja/voditelja obrade koji obrađuju osobne podatke ispitanika u svezi sa videonadzornim sustavom. 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 istog 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, 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.

U članku 83. stavku 4. točki (a) Opće uredbe o zaštiti podataka je propisano da se za kršenja obveza voditelja i izvršitelja obrade u skladu s člankom 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.

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.”.

Budući da ukupni godišnji promet na svjetskoj razini u 2019. godini za društvo Konzum plus d.o.o. iznosi 7.654.996.000,00 kn, 2% tog iznosa je 153.099.920,00 kn (20.413.322,66 EUR), a koji iznos predstavlja gornju granicu za izricanje upravne novčane kazne u konkretnom predmetu, budući da je navedeni iznos veći od 10 000 000 EUR. Navedeni podaci su javno dostupni na mrežnim stranicama FINA-e.

Agencija je radi kršenja članka 32. stavka 1. točke b) i d) te stavka 2. i 4. Opće uredbe o zaštiti osobnih podataka izrekla voditelju obrade društvu Konzum plus d.o.o. upravnu novčanu kaznu u iznosu od 675.000,00 kn, a koji iznos čini 0,44 % 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, kako je utvrđeno u točki 1. izreke ovog rješenja, došlo je do kršenja obveza izvršitelja obrade iz članka 32. stavka 1. točke b) i d) te stavka 2. i 4. Opće uredbe o zaštiti podataka, neprovođenjem odgovarajućih tehničkih mjera sigurnosti obrade osobnih podataka od strane društva Konzum plus d.o.o. kao voditelja obrade, a za koje kršenje Opća uredba o zaštiti podataka propisuje izricanje upravne novčane kazne sukladno članku 83. stavku 4. točke a), odnosno, 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 što je veće.

Sukladno Smjernicama o primjeni i određivanju upravnih novčanih kazni za potrebe Uredbe 2016/679, pokazatelj težine kršenja može biti ne samo priroda kršenja, već i opseg, svrha predmetne obrade kao i broj ispitanika i razina štete koju su pretrpjeli.

U ovoj upravnoj stvari utvrđeno je da je zaposlenik društva Konzum plus d.o.o., po uputi , voditeljice poslovnice na istoj adresi, a koja je imala pravo pristupa video zapisima, uz prisustvo treće osobe, , mobitelom snimio monitor videonadzornog sustava poslovnice na kojem je bio prikazan video zapis dvojice muškaraca starije životne dobi u fizičkom sukobu u trajanju od 50 sekundi. je učinjenu snimku zatim mobitelom proslijedio koja je istu proslijedila direktoru regije . Snimka je dospjela na društvene mreže, a 03. prosinca 2020. je objavljena i u medijima te je i dalje dostupna.

Činjenica da je lozinka za pristup videonadzornom sustavu u trenutku predmetne povrede bila vidno izvješena na rubu nadzornog monitora ukazuje da voditelj obrade nije provodio redovite kontrole propisanih mjera jer bi u suprotnom vjerojatno pravovremeno reagirao i sankcionirao odgovornu osobu za taj sigurnosni propust.

Utvrđeno je da su Konzum plus d.o.o. kao voditelj obrade i Sokol d.o.o. kao izvršitelj obrade, dana 05.07.2019. sklopili *Ugovor o obradi podataka* a 19.07.2019. sklopili *Ugovor broj* : . . . o pružanju usluga redovnog i izvanrednog održavanja sustava tehničke zaštite. Opća uredba o zaštiti podataka izravno i obvezujuće se primjenjuje u svim državama članicama od 25.05.2018. godine., iz čega proizlazi da kršenje obveza voditelja obrade glede provedbe odgovarajućih tehničkih mjera sigurnosti obrade osobnih podataka traje od 25.05.2018. te traje i dalje, odnosno, više od 3 godine jer voditelj obrade i nakon spornog incidenta nije predvidio niti implementirao odgovarajuće mjere zaštite kako bi se rizici sveli na najmanju moguću mjeru te kako bi se spriječili isti i/ili slični incidenti u budućnosti.

U predmetnoj povredi obrađivani su osobni podaci četiri ispitanika, na način da je video snimka fizičkog sukoba dvojice muškaraca na kojoj su vidljive i dvije ženske osobe učinjena dostupna javnosti putem društvenih mreža i medija zbog neprovedbe odgovarajućih mjera zaštite. Tijekom upravnog postupka nije utvrđena razina štete za ispitanike.

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

Radna skupina iz članka 29 navodi u Smjernicama o primjeni i određivanju upravnih novčanih kazni za potrebe Uredbe 2016/679 da "namjera" u pravilu uključuje znanje i nakanu u pogledu značajki prekršaja, dok "nenamjerno" znači da nije postojala namjera da se prouzroči kršenje iako je voditelj obrade/izvršitelj obrade prekršio svoju obvezu dužne pažnje propisanu zakonom. Iste Smjernice dakle naglašavaju razliku između okolnosti koje su indikativne ili „namjerne povrede“ i onih koje ukazuju na kršenja koja su prouzročena „nenamjerno“ ili „nemarom“. U tom smislu Smjernice navode "nedonošenje politika" i "ljudsku pogrešku" kao primjere ponašanja koji mogu ukazivati na nepažnju.

U odnosu na navedeno, u predmetnom slučaju nije utvrđeno da je bilo izravne namjere kršenja odredbi Opće uredbe o zaštiti podataka od strane Konzum plus d.o.o., ali je utvrđen nemar i nedostatak radnji koje bi prevenirale povredu. Naime, u ovoj upravnoj stvari utvrđeno je da se Konzum plus d.o.o. kao voditelj obrade od početka upravnog postupka poziva na implementaciju organizacijskih mjera zaštite obrade osobnih podataka (edukacije za zaposlenike i potpisivanje izjava o povjerljivosti), a iz čega se jasno može zaključiti da voditelj obrade uopće nije svjestan obveze uvođenja i implementacije odgovarajućih tehničkih mjera zaštite s obzirom na moguće rizike neovlaštenog otkrivanja osobnih podataka. Voditelj obrade očito nije bio niti svjestan mogućnosti nastanka ovakve i/ili slične povrede, a iz njegovih očitovanja proizlazi da niti nakon predmetnog incidenta nije svjestan obveze uvođenja odnosno implementacije tehničkih mjera zaštite, a čime su ispunjeni svi elementi grube nepažnje u postupanju.

Naime, voditelj obrade nije svjestan ni obveze iz članka 32. stavka 1. točke d) redovitog testiranja, ocjenjivanja i procjenjivanja učinkovitosti tehničkih i organizacijskih mjera za osiguravanje sigurnosti obrade, a čime su ispunjeni svi elementi grube nepažnje u postupanju. Naime da je voditelj obrade procjenjivao učinkovitosti tehničkih i organizacijskih mjera za osiguravanje sigurnosti obrade sukladno članku 32. stavka 1. točke d) Opće uredbe o zaštiti podataka, primjerice provjerom poslovne opravdanosti ostvarenih uvida u snimke videonadzornog sustava, zaposlenici se ne bi tako olako kršili propisana interna pravila društva te bi se na taj način znatno umanjio rizik od neovlaštene obrade osobnih podataka ispitanika od strane zaposlenika voditelja obrade.

Osim navedenoga, voditelj obrade je mogao implementirati i druge tehničke mjere zaštite osobnih podataka, a kojima se mogla prevenirati navedena povreda. Primjerice, mogao je organizirati odnosno implementirati sigurnosni sustav naknadnog pregledavanja snimki baziran na „sumnji u sigurnosni incident“ (npr. krađa, tjelesni napadi, prijetnje) na način da se uvid u nastale snimke provodi uz znanje i odobrenje za to posebno ovlaštene osobe izvršitelja obrade, a čime bi se osigurala dodatna i primjerena mjera autorizacije pristupa pohranjenim

snimkama koja bi znatno umanjila rizik od neovlaštene obrade osobnih podataka ispitanika od strane zaposlenika voditelja obrade. Dakle, moguća je implementacija automatskog signaliziranja od strane sustava naknadnog pregledavanja snimki, kao procedure dodatne provjere poslovne uvjetovanosti/opravednosti takvog postupanja gdje bi bilo obvezujuće provjeriti tj. opravdati/potvrditi od strane kontrolne razine takve radnje u sustavu.

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

Nastavno na predmetnu povredu, voditelj obrade nije poduzeo odgovarajuće tehničke mjere sigurnosti obrade osobnih podataka, a koje bi rizike neovlaštenog otkrivanja osobnih podataka svele na najmanju moguću mjeru. Isto tako, potrebno je naglasiti da navedeno društvo nije poduzelo niti druge moguće radnje kako bi se umanjio navedeni rizik koji je prouzročen opisanom incidentom, a koji je doveo do objave osobnih podataka ispitanika u medijima i na društvenim mrežama, primjerice, nije poduzeo radnje usmjerene u pravcu uklanjanja sporne snimke s društvenih mreža odnosno iz medija.

- 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):

Uzimajući u obzir odredbe članka 32. koje obvezuju voditelja obrade i izvršitelja obrade da provode odgovarajuće tehničke i organizacijske mjere kako bi osigurali odgovarajuću razinu sigurnosti s obzirom na rizik, uključujući prema potrebi: sposobnost osiguravanja trajne povjerljivosti, cjelovitosti, dostupnosti i otpornosti sustava i usluga obrade; proces za redovno testiranje, ocjenjivanje i procjenjivanje učinkovitosti tehničkih i organizacijskih mjera za osiguravanje sigurnosti obrade, da se prilikom procjene odgovarajućeg nivoa sigurnosti posebno uzimaju rizici koje predstavlja obrada, posebno rizici od slučajnog ili nezakonitog uništenja, gubitka, izmjene, neovlaštenog otkrivanja osobnih podataka, ili neovlaštenog pristupa osobnim podacima koji su preneseni, pohranjeni ili na drugi način obrađivani, te da voditelj 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, utvrđeno je da Konzum plus d.o.o. provodi određene organizacijske mjere zaštite (edukacija zaposlenika i potpisivanje izjave o povjerljivosti), da je usvojio interne akte kojima se regulira zaštita osobnih podataka dok tehničke i organizacijske mjere nisu odgovarajuće te također nisu predmet redovite provjere. Također, uvidom u sporni video zapis utvrđeno je da je u trenutku nastanka povrede, lozinka za pristup videonadzornom sustavu bila vidno izvješena na rubu monitora što se također smatra propustom u mjerama zaštite sustava pohrane predmetnog videonadzornog sustava, koji za posljedicu može imati neovlašteni pristup učinjenim snimkama/video zapisima.

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

Prema evidencijama kršenja koje vodi ova Agencija, društvo Konzum plus d.o.o. u prošlosti je počinilo kršenje Opće uredbe o zaštiti podataka za što je Agencija donijela Rješenje KLASA:

URBROJ: od 13. siječnja 2020. a u kojem je utvrđeno da je društvo Konzum plus d.o.o. iz Zagreba Marijana Čavića 1A, trgovina Konzum Maxi u Novom Marofu, Moždenec 1/K, dana 12. listopada 2018. omogućila zaposlenici

neovlašteni pristup osobnim podacima ispitanika putem uvida u snimke videonadzornog sustava protivno članku 28. stavku 1. i 3. Zakona o provedbi Opće uredbe o zaštiti podataka, a koje je kršenje ova Agencija cijenila kao otegotnu okolnost prilikom utvrđenja visine upravne novčane kazne.

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

Društvo Konzum plus d.o.o. 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);

Na predmetnom video zapisu mogu se jasno razabrati crte lica, konstitucija, pokreti tijela te ostale fizičke značajke ispitanika koje je moguće izravno povezati s pojedincima.

- 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);

Člankom 33. stavkom 1. Opće uredbe o zaštiti podataka propisano je da voditelj obrade bez nepotrebnog odgađanja izvješćuje nadzorno tijelo nakon što sazna za povredu osobnih podataka. Za predmetnu povredu nadzorno tijelo je saznalo putem zaprimljenog *Izvješća o povredi osobnih podataka* koje je dostavilo društvo Konzum plus d.o.o. kao voditelj obrade.

- 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);

Društvu Konzum plus d.o.o. 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);

Nije utvrđeno da je Konzum plus d.o.o. ostvario financijsku dobit kršenjem niti izbjegnuo gubitke, izravno ili neizravno. Međutim, Agencija otegotnu okolnost nalazi u činjenici da voditelj obrade nije uložio napor upućivanjem zahtjeva za uklanjanje spornog video zapisa sa javno dostupnih medija.

Dok su pojmovi „osobni podaci“, „ispitanik“, „voditelj obrade“ i „izvršitelj obrade“ definirani Općom uredbom o zaštiti podataka, pojam „osobe koje su ovlaštene za obradu osobnih podataka pod izravnom nadležnošću voditelja obrade ili izvršitelja obrade“ nije. Međutim, općenito se podrazumijeva da se taj pojam odnosi na osobe koje pripadaju pravnoj osobi voditelja ili izvršitelja obrade, ali samo u onoj mjeri ukoliko su ovlašteni na obradu osobnih podataka. Zaposlenik koji ostvari pristup osobnim podacima za koji pristup nije ovlašten i u svrhu različitu od svrhe poslodavca ne potpada u tu kategoriju. Umjesto toga, taj zaposlenik treba se smatrati trećom stranom u odnosu na obradu podataka koju poduzima poslodavac. Ukoliko zaposlenik obrađuje osobne podatke u svoju svrhu (za svoje potrebe), različitu od svrhe poslodavca, zaposlenik treba biti smatran voditeljem obrade i preuzeti na sebe sve posljedice i obveze koje proizlaze iz obrade osobnih podataka. Poslodavac (kao inicijalni voditelj obrade) bi neovisno o navedenome mogao zadržati određenu odgovornost u slučaju da je do nove obrade došlo zbog nedostatka sigurnosnih mjera.

Zaključno, Agencija je u ovom upravnom postupku utvrdila da je voditelj obrade Konzum Plus d.o.o. iz Zagreba, Ulica Marijana Čavića 1/a propustio provesti odgovarajuće mjere sigurnosti obrade sukladno postojećim i predvidivim rizicima, redovito nadzirao učinkovitost provedbe trenutnih tehničkih i organizacijskih mjera, čime je postupio protivno odredbama članka 32., stavka 1. točke b) i d) i stavka 2. i 4. Opće uredbe o zaštiti podataka, što je dovelo do neovlaštene obrade osobnih podataka ispitanika objavom u medijima i na društvenim mrežama.

Dakle, Agencija je izrekla upravnu novčanu kaznu zbog nepoduzimanja odgovarajućih tehničkih i organizacijskih mjera koje je sukladno navedenoj odredbi Opće uredbe o zaštiti podataka obvezan poduzeti voditelj obrade, a uslijed čega je došlo do neovlaštene obrade osobnih podataka ispitanika njihovom javnom objavom na društvenim mrežama i u medijima, a ne za samu neovlaštenu obradu osobnih podataka ispitanika, odnosno za njihovu objavu na društvenim mrežama i u medijima. Upravo nepoduzimanjem odgovarajućih tehničkih i organizacijskih mjera zaštite voditelj obrade nije spriječio svog zaposlenika da neovlašteno obrađuje osobne podatke ispitanika čime mu je zapravo posredno omogućio takvu neovlaštenu obradu. Europski odbor za zaštitu podataka, jednako kao i Rezolucija o ulozi ljudske pogreške u povredama osobnih podataka 41. Međunarodne konferencije povjerenika za zaštitu podataka i privatnosti iz 2019. godine, ističe da adekvatne mjere sigurnosti moraju biti poduzete kako bi se spriječile ljudske pogreške.

Agencija je provela ispitni postupak sukladno člancima 51. i 52. Zakona o općem upravnom postupku (u daljnjem tekstu: ZUP) 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 društvo Konzum plus d.o.o. 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 odvrćajuća 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 Zagrebu u roku od 30 dana od dana dostave rješenja.

RAVNATELJ
Zdravko Vukić, mag.oec.



Dostaviti:

1. Konzum plus d.o.o Ulica Marijana Čavića 1/A, (AR)
2. Pismohrana, ovdje