REPUBLIKA E SHQIPËRISË
KOMISIONERI PËR TË DREJTËN E INFORMIMIT DHE MBROJTJEN E TË DHËNAVE PERSONALE
DREJTORIA PËR MBROJTJEN E TË DHËNAVE PERSONALE

Nr. 377/6 prot. Tiranë më 18.6.2020

REKOMANDIM

Nr. 12, datë 18.6.2020

PËR KONTROLLUESIN "*TRAVEL SERVICES*" SHPK

Në mbështetje të neneve 29, 30 dhe 32 të ligjit nr. 9887, datë 10.03.2008 "*Për mbrojtjen e të dhënave personale*" i ndryshuar (në vijim "*Ligji*"), ligjit nr. 44/2015 "*Kodi i Procedurave Administrative të Republikës së Shqipërisë*" (në vijim "*Kodi i Procedurave Administrative*"), procesverbalit të hetimit administrativ dhe provave të administruara në ngarkim të kontrolluesit "*Travel Services*" SHPK,

KONSTATOVA SE:

Në zbatim të Urdhrit nr. 62, datë 06.03.2020 të Komisionerit për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale, u krye hetimi administrativ pranë kontrolluesit "*Travel Services*" SHPK, me objekt:

- Zbatimi i ligjit nr. 9887, datë 10.03.2008 "*Për mbrojtjen e të dhënave personale*" i ndryshuar dhe akteve të miratuara nga Komisioneri në lidhje me mbledhjen, përpunimin, ruajtjen dhe sigurinë e të dhënave personale, gjatë kryerjes së aktivitetit nga ana e kontrolluesit.

Zyra e Komisionerit, pasi shqyrtoi relacionin e hetimit administrativ, procesverbalin e konstatimit dhe provat e administruara gjatë ushtrimit të hetimit, vëren se:

1. Kontrolluesi "*Travel Services*" SHPK (në vijim, "*Kontrolluesi*") ushtron veprimtari në fushën e menaxhimit dhe promocionit të aktivitetit turistik në përgjithësi, si dhe, në mënyrë të veçantë, udhëtimeve në anije turistike (krociera);

2. Kontrolluesi përpunon të dhëna personale për kategoritë e subjekteve të të dhënave punëmarrës, kandidatë për punë, si dhe klientë. Kontrolluesi nuk ka parashikuar afate konkrete për përpunimin e të dhënave personale dhe sensitive për kategorinë punëmarrës, kandidatë për punë dhe klientë, në kundërshtim me parashikimet në germën "d" të pikës 1 të nenit 5 të Ligjit.

Zyra e Komisionerit vlerëson se Kontrolluesi ka detyrimin të përpunojë të dhënat personale për aq kohë sa ekziston qëllimi për të cilin janë përpunuar të dhënat personale. Në momentin që qëllimi ka përfunduar është e nevojshme që Kontrolluesi, vetë ose nëpërmjet delegimit te një palë e tretë në cilësinë e përpunuesit, të realizojë shkatërrimin e tyre, në të kundërt përpunimi i mëtejshëm i të dhënave konsiderohet i paligjshëm;

3. Kontrolluesi ka nënshkruar një kontratë, për mirëmbajtjen e faqes së internetit dhe hostimin, me shoqërinë "*Matrix Digital LLC*", e cila është një shoqëri e themeluar dhe organizuar sipas legjislacionit të Republikës së Kosovës.
   Nga analizimi i "Formularit të Njoftimit" të depozituar nga Kontrolluesi, rezulton se ky i fundit nuk ka njoftuar Zyrën e Komisionerit lidhur me transferimin e të dhënave personale në Republikën e Kosovës. Në këtë kuadër, në referim të nenit 9 të Ligjit, rezulton se Kontrolluesi nuk ka paraqitur kërkesë për autorizim, nga Zyra e Komisionerit, përpara transferimit të të dhënave personale;

4. Nga analizimi i Kontratës me shoqërinë "*Matrix Digital LLC*", rezulton se, në nenin 12 të saj, është parashikuar një dispozitë e përgjithshme për ruajtjen e privatësisë, por nuk janë reflektuar detyrat dhe përgjegjësitë e palëve, masat teknike dhe organizative, sipas parashikimeve të nenit 20 të Ligjit dhe Udhëzimit nr. 19, datë 03.08.2012, të Komisionerit "*Mbi rregullimin e marrëdhënieve mes kontrolluesit dhe përpunuesit në rastet e delegimit të përpunimit të të dhënave dhe përdorimin e një kontrate tip në rastet e këtij delegimi*" i ndryshuar (në vijim, "*Udhëzimi nr. 19*").

   Gjithashtu, Kontrolluesi ka nënshkruar një kontratë me shoqërinë "*SIGAL UNIQA GROUP AUSTRIA*" SHA, për sigurimin e jetës dhe shëndetit të punëmarrësve.
   Nga analizimi i kontratës, rezulton se nuk janë parashikuar detyrimet e palëve sipas të nenit 20 të Ligjit dhe Udhëzimit nr. 19.

   Zyra e Komisionerit e vlerëson si shumë të rëndësishëm parashikimin e detyrimeve midis kontrolluesit dhe përpunuesve, në rastet e delegimit të shërbimeve, sa i përket parashikimit të kushteve teknike dhe organizative dhe masave të sigurisë, konfidencialitetit, garantimin e të drejtave të subjekteve dhe se çfarë do të ndodhë me të dhënat personale të përpunuara, pas përfundimit të efekteve ligjore të kontratës;

5. Nga verifikimi i regjistrit të kontrolluesve, protokollit të Zyrës së Komisionerit, si dhe deklarimet e përfaqësuesve të kontrolluesit, rezulton se Kontrolluesi nuk ka njoftuar në lidhje me përpunimin e të dhënave personale, për të cilat është përgjegjës, në zbatim të nenit 21 të Ligjit.

   Kontrolluesi ka depozituar "Formularin e Njoftimit", pranë Zyrës së Komisionerit, pas fillimit të hetimit administrativ, më datë 09.03.2020.

Pikën 1 e nenit 21 të Ligjit parashikon se njoftimi duhet të bëhet para se kontrolluesi të përpunojë të dhënat për herë të parë ose kur kërkohet ndryshimi i gjendjes së njoftimit të përpunimit të njoftuar më parë.

Në bazë të të dhënave të ekstraktit të tregtar, të publikuar në Qendrën Kombëtare të Biznesit, rezulton se Kontrolluesi është themeluar dhe ushtron veprimtarinë e tij që prej datës 28.10.2019.

Pika 1 e nenit 25 të Ligjit parashikon se Kontrolluesi nuk mund të fillojë përpunimin e të dhënave personale pa njoftuar më parë Zyrën e Komisionerit.

Në këto kushte, konsiderohet shkelje serioze e legjislacionit për mbrojtjen e të dhënave personale përpunimi i të dhënave personale, pa njoftuar dhe pa u regjistruar më parë, në regjistrin elektronik të subjekteve kontrolluese, të administruar nga Zyra e Komisionerit.

Zyra e Komisionerit vlerëson se realizimi i detyrimit për njoftim është i rëndësishëm, pasi i jep mundësinë subjekteve të të dhënave që të informohen për përpunimin e dhënave të tyre, si dhe realizimin e detyrimeve ligjore të Kontrolluesit. Kjo i jep mundësi reale subjekteve të të dhënave për të ushtruar të drejtat e tyre sipas ligjit;

6. Kontrolluesi ka parashikuar, në dokumentin "*Privacy Policy*", disa rregulla të përgjithshme për mënyrën e përpunimit të të dhënave personale, me fokus kategorinë e subjekteve të të dhënave "*klientë*", por nuk ka hartuar një rregullore specifike për mbrojtjen e të dhënave, në mënyrë që të parashikojë masa teknike dhe organizative për çdo proces përpunues dhe për çdo kategori subjektesh të të dhënave.

   Konkretisht në këtë dokument, nuk parashikohen rregulla teknike dhe organizative për përpunimin e të dhënave për kategorinë e subjekteve të të dhënave punëmarrës dhe kandidatë për punë, në kundërshtim me nenin 27 të Ligjit.

   Zyra e Komisionerit vlerëson se hartimi i një "*Rregulloreje specifike për mbrojtjen, përpunimin, ruajtjen dhe sigurinë e të dhënave personale*", në të cilën të parashikohen rregulla dhe procedura organizative specifike mbi mënyrën e përpunimit të të dhënave personale (për çdo kategori subjekti të dhënash), sigurinë e të dhënave, konfidencialitetin, afatet e mbajtjes së të dhënave, etj., konsiderohet një detyrim shumë i rëndësishëm në zbatim të nenit 27 të Ligjit, pasi shmang pasojat e rënda që mund të vijnë për subjektet e të dhënave.

   Kjo rregullore duhet të jetë gjithëpërfshirëse, duke përfshirë çdo lloj përpunimi të të dhënave personale të Kontrolluesit për çdo kategori subjektesh të të dhënave, sipas deklarimeve në "Formularin e Njoftimit";

7. Kontrolluesi bën pjesë në kategorinë e subjekteve përpunuese të mëdhenj në kuptim të Udhëzimit nr. 47, datë 14.09.2018, të Komisionerit "*Për përcaktimin e rregullave*

për ruajtjen e sigurisë së të dhënave personale të përpunuara nga subjektet përpunuese të mëdha" (në vijim, "*Udhëzimi nr. 47*)".

Kontrolluesi nuk ka marrë masa në kuadër të trajnimit të punonjësve që kanë akses dhe përpunojnë të dhëna personale, lidhur me legjislacionin në fuqi për mbrojtjen e të dhënave personale, si dhe vërehet mosplotësim i detyrimeve në lidhje me ngritjen, administrimin dhe mirëmbajtjen e sistemit të menaxhimit së sigurisë së informacionit (SMSI) lidhur me mbrojtjen e të dhënave personale, të parashikuara nga Udhëzimi nr. 47, datë 14.09.2018 të Komisionerit "*Për përcaktimin e rregullave për ruajtjen e sigurisë së të dhënave personale të përpunuara nga subjektet përpunuese të mëdha*".

Zyra e Komisionerit vlerëson se, për shkak të cilësisë si subjekt përpunues i madh, si dhe për shkak të natyrës së veprimtarisë që ushtron, e cila kërkon masa të shtuara teknike dhe organizative për garantimin e sigurisë së të dhënave personale, Kontrolluesi është i detyruar të krijojë, mirëmbajë dhe administrojë SMSI në përputhje me parashikimet e Udhëzimit nr. 47.

SMSI për mbrojtjen e të dhënave personale duhet të bazohet në standardin ISO/IEC 27001, siç parashikohet nenin 5 të Udhëzimit nr. 48, datë 14.09.2018, të Komisionerit "*Për certifikimin e sistemeve të sigurisë së informacionit, të dhënave personale dhe mbrojtjes së tyre*" (në vijim, "*Udhëzimi nr. 48*"), si dhe është një sistem i certifikueshëm për qëllime përputhshmërie me standardin e sipërpërmendur, vetëm nga organizma të akredituar dhe autorizuar sipas parashikimeve të Udhëzimit 48.

Në përfundim të hetimit administrativ, referuar provave dhe konstatimeve në vend, grupi i hetimit administrativ hartoi procesverbalin përkatës dhe, në respektim të së drejtës për t'u dëgjuar, në zbatim të neneve 87-89 të Kodit të Procedurave, më datë 16.06.2020, u mbajt një seancë dëgjimore në praninë e përfaqësuesit të autorizuar të Kontrolluesit.

Gjatë seancës dëgjimore, përfaqësuesi i autorizuar i Kontrolluesit deklaroi se ka marrë, si dhe po vijon të marrë, masa në drejtim të rikuperimit të mangësive të konstatuara gjatë hetimit administrativ.

Më tej, përfaqësuesi i Kontrolluesit paraqiti sqarimet si vijon:

- Lidhur me marrëdhënien kontraktore të Kontrolluesit me shoqërinë "*Matrix Digital LLC*", për mirëmbajtjen e faqes së internetit dhe hostimin, përfaqësuesi i Kontrolluesit deklaroi se shoqëria në fjalë i ka deleguar shërbimet për Kontrolluesin tek shoqëria "*Albanian Telecommunication Information Services*" SHPK, nëpërmjet kontratës së bashkëpunimit, të datës 03.01.2020.

  Nga analizimi i përmbajtjes së kësaj kontratës në fjalë, të vënë në dispozicion gjatë seancës dëgjimore, Zyra e Komisionerit nuk konstaton dispozita të shprehura lidhur me delegimin e shërbimeve.

- Në lidhje me konstatimet e tjera të Zyrës së Komisionerit, përfaqësuesi i autorizuar i Kontrolluesit, u shpreh se ky i fundit, nisur nga prania relativisht e re në treg, kërkon një kohë të arsyeshme për të ndrequr konstatimet e Zyrës së Komisionerit në kuadër të hetimit administrativ.

Zyra e Komisionerit vlerëson bashkëpunimin e Kontrolluesit me grupin e hetimit administrativ dhe angazhimin e tij për të rikuperuar shkeljet e konstatuara. Plotësimi i këtyre detyrimeve nga ana e Kontrolluesit është mjaft i rëndësishëm pasi garanton përpunimin e ligjshëm, sigurinë e të dhënave personale dhe eviton mundësinë e përhapjes së tyre në mënyrë të paligjshme.

Sa më sipër, në zbatim të neneve 5, 9, 20, 21, 27, 29, 30, 31 (pika 1, gërma "a/1"), si dhe 32 të Ligjit,

REKOMANDOJ:

1. Kontrolluesi të ketë në vëmendje të vazhdueshme përpunimin e të dhënave personale në përputhje me dispozitat e parashikuara në nenin 5 të Ligjit, si dhe të marrë masa për adresimin e konstatimeve të Komisionerit në lidhje me shkelje të kësaj dispozite. Për këtë arsye, Kontrolluesi të parashikojë afate konkrete për ruajtjen e të dhënave personale për kategoritë e subjekteve të dhënat personale të të cilëve ai përpunon sipas parashikimeve të nenit 5 të Ligjit. Për këto afate të informohen edhe subjektet e të dhënave;

2. Kontrolluesi të saktësojë marrëdhënien e delegimit të përpunimit për krijimin dhe mirëmbajtjen e faqes web dhe përcaktimin e përpunuesit, dhe nëse rezulton se janë transferuar të dhëna personale në Kosovë, të kryejë shkatërrimin e menjëhershëm të tyre;

3. Kontrolluesi të përfshijë në marrëveshjet me përpunuesit përkatës, detyrimet sipas parashikimeve të nenit 20 të Ligjit dhe Udhëzimit nr. 19;

4. Kontrolluesi, në zbatim të neneve 21 dhe 22 të Ligjit, të ketë në vëmendje të vazhdueshme përditësimin e "*njoftimit*" në lidhje me ndryshimin e gjendjes së përpunimit të të dhënave personale, të cilat përpunon;

5. Kontrolluesi, në zbatim të nenit 27 të Ligjit, të hartojë një rregullore të posaçme, në të cilën të parashikohen masa konkrete teknike dhe organizative për mbrojtjen e të dhënave personale, në përputhje me veprimtarinë dhe proceset përpunuese që kryen;

6. Kontrolluesi, me qëllim garantimin e sigurisë së të dhënave personale, të zbatojë detyrimet e përcaktuara në të Udhëzimit nr. 47, lidhur me trajnimin e stafit të tij, si dhe sa i përket krijimit, mirëmbajtjes dhe administrimit të Sistemit të Menaxhimit të Sigurisë së Informacionit (SMSI) për mbrojtjen e të dhënave personale.

SMSI për mbrojtjen e të dhënave personale duhet të krijohet në përputhje me standardin ISO/IEC 270001, siç parashikohet në nenin 5 të Udhëzimit nr. 48, si dhe mund të certifikohet, për qëllime përputhshmërie me standardin në fjalë, nga organizma të akredituar dhe autorizuar në përputhje me dispozitat e këtij udhëzimi. Në këtë rast, Kontrolluesi, në zbatim të germës "b" të pikës 42 të Udhëzimit nr. 47, depoziton pranë Zyrës së Komisionerit një kopje të certifikatës së përputhshmërisë;

7. Në zbatim të pikës 1 të nenit 32 të Ligjit, të përmbushen brenda 30 ditëve detyrimet e treguara në pikat 1 deri 5 më sipër, si dhe brenda 60 ditëve detyrimi i treguar në pikën 6.

   Afatet e sipërpërmendura fillojnë nga data marrjes dijeni të këtij akti;

8. Kontrolluesi të njoftojë Komisionerin për masat e marra.

   Në rast mospërmbushjeje të detyrimeve të parashikuara në këtë akt, Komisioneri vepron sipas pikës 2 të nenit 30 dhe nenit 39 të Ligjit, të cilët parashikojnë se në rast shkeljesh serioze, të përsëritura ose të qëllimshme të Ligjit nga një kontrollues ose përpunues, veçanërisht në rastet e përsëritura të moszbatimit të rekomandimeve të tij, Komisioneri vendos sanksione administrative për kundërvajtjet administrative përkatëse dhe e denoncon publikisht ose e raporton çështjen në Kuvend dhe në Këshillin e Ministrave.

Ky Rekomandim u shpall sot, më datë 18.6.2020

KOMISIONERI

Besnik Dervishi