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

Nr. 291/2 prot. Tiranë më 18.6.2020

REKOMANDIM

Nr. 08, datë 18.6.2020

PËR KONTROLLUESIN "*MICRO CREDIT RISK*" 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 "*Micro Credit Risk*" SHPK,

KONSTATOVA SE:

Në zbatim të Urdhrit 46, datë 26.02.2020 të Komisionerit për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale, u krye hetimi administrativ pranë kontrolluesit "*Micro Credit Risk*" 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 "*Micro Credit Risk*" SHPK (në vijim, "*Kontrolluesi*") është një subjekt financiar jobankë që ushtron veprimtari, ndër të tjera, në fushën e kredidhënies, faktoringut, etj., në përputhje me legjislacionin në fuqi;

2. Kontrolluesi përpunon të dhëna personale për kategorinë e subjekteve të të dhënave punëmarrës, të tilla si emër, mbiemër, numër telefoni, e-mail, numër i sigurimit shoqëror, numri personal i identifikimit, jeta profesionale, arsimi, të dhëna shëndetësore, adresa, fotografi, etj.

   Kontrolluesi nuk ka parashikuar afate konkrete për mbajtjen dhe përpunimin e të dhënave personale të punëmarrësve, pas largimit të tyre dhe përfundimit të

marrëdhënies së punës, në kundërshtim me parashikimet në germën "d" të pikës 1 të nenit 5 të Ligjit dhe me Udhëzimin nr. 11, datë 08.09.2011, të Komisionerit, "*Për përpunimin e të dhënave të punonjësve në sektorin privat*" i ndryshuar (në vijim, "*Udhëzimi nr. 11*").

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 disponon faqen e internetit https://krediajuaj.eu/.

Nga analizimi i saj, që në faqen e parë, rezultoi se nuk ekzistonte një rubrikë në lidhje me "*Politikat e Privatësisë*", e cila ishte e aksesueshme vetëm nëpërmjet rubrikës së kërkimit.

Rrjedhimisht, kjo rubrikë nuk ishte lehtësisht e dukshme dhe e aksesueshme duke bërë të pamundur realizimin e informimit të qytetarëve, në zbatim të nenit 18 të Ligjit.

Në vijim, pas hetimit administrativ, u konstatua se kontrolluesi reagoi menjëherë duke i vendosur "*Politikat e Privatësisë*" në një vend të dukshëm.

Zyra e Komisionerit vlerëson se informimi i subjekteve të të dhënave personale është një nga detyrimet bazë të Kontrolluesit, pasi iu mundëson atyre të njihen me të drejtat që iu janë akorduar në Kushtetutë dhe Ligj, si dhe iu mundëson, gjithashtu, ushtrimin e këtyre të drejtave në praktikë. Mospërmbushja e këtij detyrimi, nga ana e Kontrolluesit, mund të sjellë pasoja të rënda sa i përket jetës private dhe, bashkë me të, të drejtës së subjekteve të të dhënave për mbrojtjen e të dhënave personale të tyre.

4. Kontrolluesi ka nënshkruar një kontratë me shoqërinë "*DATECH*" SHPK , me objekt ndërtimin dhe mirëmbajtjen e një sistemi për përpunimin e të dhënave financiare të klientëve, në kuadër të ofrimit të shërbimeve financiare.

Nga analizimi i dispozitave të kontratës në fjalë rezulton se 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*").

Zyra e Komisionerit e vlerëson si shumë të rëndësishëm parashikimin e detyrimeve midis kontrolluesit dhe përpunuesit, 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 nga hetimi administrativ i ushtruar, rezultoi se Kontrolluesi e ka përmbushur detyrimin për njoftim në zbatim të nenit 21 të Ligjit.

   Nga ana tjetër, nga analizimi i përmbajtjes së njoftimit, në raport me proceset përpunuese dhe dokumentacionin e administruar gjatë procesit të hetimit administrativ, rezulton se nuk është përditësuar përmbajtja e tij, sa i përket kategorive të tjera të subjekteve të të dhënave (kategoria punëmarrës), si dhe sa i përket rubrikave të tjera që lidhen me këtë përpunim.

   Gjithashtu nuk është reflektuar në rubrikën 7 "*Marrësit e të dhënave personale*" përhapja dhe transmetimi i të dhënave personale për këto kategori subjektesh dhe për përpunuesit e kontraktuar nga kontrolluesi.

   Nga analizimi i "*rregullores për mbrojtjen, përpunimin dhe ruajtjen e sigurisë së të dhënave personale*" (që Kontrolluesi e ka emërtuar "*Politika për mbrojtjen e të dhënave personale*") rezultojnë të dhëna lidhur me proceset përpunuese që nuk reflektohen në "Formularin e Njoftimit", me konkretisht:

   (i) Në pikën 1, të saj Kontrolluesi deklaron se transferon të dhëna te palët e treta;

   (ii) Në pikën 2, është parashikuar promovimi i produkteve financiare duke përdorur të dhëna personale si numër telefoni dhe adresë e-mail (aktivitet marketingu), duke parashikuar mundësinë, e transferimit të këtyre të dhënave në call-center.

   Zyra e Komisionerit vlerëson se realizimi i detyrimit për përditësimin e njoftimit është i rëndësishëm, pasi i jep mundësinë subjekteve të të dhënave që të informohen për përpunimin e të dhënave të tyre, që kryen Kontrolluesi, si dhe për realizimin e detyrimeve ligjore të Kontrolluesit. Kjo ju jep mundësi reale subjekteve të të dhënave për të ushtruar në mënyrë korrekte të drejtat e tyre sipas ligjit.

6. Rregullorja e hartuar nga Kontrolluesi (e emërtuar "*Politika për mbrojtjen e të dhënave personale*") rezulton të jetë sipas standardit të rregullores të publikuar në faqen zyrtare të Zyrës së Komisionerit, www.idp.al.

   Kjo rregullore, pavarësisht faktit se referon në disa procese përpunuese (përpunim i të dhënave të klientëve, përpunim i të dhënave të punëmarrësve, përpunim për qëllime marketingu, etj.) ka karakter të përgjithshëm dhe nuk përmbush kërkesat dhe detyrimet ligjore për parashikimin e rregullave specifike për mbrojtjen e të dhënave personale në referim të akteve nënligjore specifike të miratuara nga Zyra e Komisionerit.

Zyra e Komisionerit vlerëson se hartimi i një rregulloreje të posaçme për mbrojtjen, përpunimin, ruajtjen dhe sigurinë e të dhënave personale, në të cilën të parashikohen rregulla dhe procedura organizative specifike për mënyrën e përpunimit të të dhënave personale (për çdo kategori subjektesh të të dhënave), sigurinë e të dhënave, konfidencialitetin, afatet e mbajtjes së të dhënave, etj., konsiderohet një detyrim mjaft 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 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 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 "*Për përcaktimin e rregullave për ruajtjen e sigurisë së të dhënave personale të përpunuara nga subjektet përpunuese të mëdha*" (në vijim, "*Udhëzimi nr. 47*").

   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 nr. 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 Kontrolluesit.

Gjatë seancës dëgjimore, përfaqësuesi i Kontrolluesit deklaroi se ka paraqitur pretendimet e tij me shkrim.

Sa i përket pretendimeve të Kontrolluesit, Zyra e Komisionerit vlerëson se:

- Në lidhje me mungesën e parashikimit të afateve të përpunimit të të dhënave, pretendimi i kontrolluesit, Zyra e Komisionerit vlerëson se pretendimi dhe referenca

në nenin 33 të Kodit të Punës nuk qëndron, pasi dispozitat e nenit në fjalë nuk janë shteruese në lidhje me afatet e përpunimit. Konkretisht, në paragrafin 5 të nenit 33 parashikohet detyrimi i Kontrolluesit për të marrë pëlqimin e punëmarrësit në lidhje me përpunime të mëtejshme të të dhënave personale të këtij të fundit, pas përfundimit të marrëdhënies së punës.
Gjithashtu, dispozitat e nenit në fjalë nuk derrogojnë detyrimet e Kontrolluesit të cilat burojnë nga dispozitat e Ligjit dhe akteve nënligjore të nxjerra në zbatim të tij.

Njoftimi për afatin e ruajtjes së të dhënave personale duhet të jetë i drejtpërdrejtë dhe i qartë për subjektin e të dhënave, si dhe i shoqëruar më informacione të tjera shtesë që kanë të bëjnë me të drejtat që gëzon subjekti i të dhënave (në këtë rast, punëmarrësi) lidhur, ndër të tjera, edhe me faktin se çfarë ndodh me të dhënat pas mbarimit të afati të ruajtjes së tyre (pra nëse të dhënat shkatërrohen, si dhe mënyrën sesi shkatërrohen, apo nëse ato i kthehen subjektit të të dhënave, duke përcaktuar edhe mënyrën për këtë qëllim).

- Në lidhje me mosvendosjen e politikës së privatësisë në një vend të dukshëm në faqen e internetit, të cilën Kontrolluesi e ka kundërshtuar në provat e paraqitura (nëpërmjet imazhit të printuar të faqes së internetit), Zyra e Komisionerit konstaton se Kontrolluesi ka kryer korrigjimin për këtë qëllim, pas hetimit administrativ.

- Në lidhje me pretendimin e kontrolluesit se neni 20 i Ligjit nuk zbatohet në kontratën e shërbimit ndërmjet Kontrolluesit dhe shoqërisë "DATECH" SHPK, sepse kontrata është e kufizuar vetëm në krijimin e programit kompjuterik (*software*) dhe nuk ka përpunim të dhënash, Zyra e Komisionerit konstaton se aksesi i ofruesit të shërbimit në të dhënat e Kontrolluesit është i parashikuar konkretisht në pikat 4.4 (*Transferimi i të dhënave*) dhe 4.6 (*Garancia dhe mirëmbajtja pas garancisë*) të kontratës.

- Sa i përket përditësimit të "Formularit të Njoftimit", Kontrolluesi ka deklaruar se do ta rishikojë atë duke përditësuar rubrikat e konstatuara si të paplota nga Zyra e Komisionerit.

- Në lidhje me pretendimin e Kontrolluesit se rregullorja ("*Politika për mbrojtjen e të dhënave*") është hartuar në përputhje të plotë me nenin 27 të ligjit, Zyra e Komisionerit vlerëson se dokumenti i mësipërm nuk është në përputhje me nenin 27, në tërësinë e tij. Konstatohet se janë ruajtur dispozita të modelit standard, të cilat nuk zbatohen në proceset përpunuese të Kontrolluesit.

  Rregullorja 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".

- Në lidhje me Sistemin e Menaxhimit të Sigurisë së Informacionit (SMSI), Kontrolluesi deklaron se ka ndërmarrë hapat e nevojshëm për implementimin e tij,

por nuk ka paraqitur prova dhe dëshmi për një pretendim të tillë. Gjithashtu, nuk janë dokumentuar as trajnimet e punonjësve që kanë akses në të dhënat personale.

- Më tej, përfaqësuesi i Kontrolluesit deklaroi se ka marrë, si dhe po vijon të marrë, masa në drejtim të rikuperimit të plotë të mangësive të konstatuara gjatë 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, 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 përfshijë në marrëveshjen me përpunuesin "*DATECH*" SHPK , detyrimet sipas parashikimeve të nenit 20 të Ligjit dhe Udhëzimit nr. 19.

3. 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;

4. Kontrolluesi, në zbatim të nenit 27 të Ligjit, të përditësojë dhe saktësojë rregulloren 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;

5. 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;

6. Në zbatim të pikës 1 të nenit 32 të Ligjit, të përmbushen brenda 30 ditëve detyrimet e treguara në pikat 1 deri 4 më sipër, si dhe brenda 60 ditëve detyrimi i treguar në pikën 5.

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

7. 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