



REPUBLIKA E SHQIPËRISË
KOMISIONERI PËR TË DREJTËN E INFORMIMIT DHE MBROJTJEN E TË
DHËNAVE PERSONALE
DREJTORIA E PËRGJITHSHME PËR MBROJTJEN E TË DHËNAVE PERSONALE
DREJTORIA E HETIMIT SEKTORIAL DHE SIGURISË SË TË DHËNAVE

Nr. 541 prot.

Tiranë, më 30.01.2025

REKOMANDIM

Nr. 01, datë 30.01.2025

PËR KONTROLLUESIN “BANKA E BASHKUAR E SHQIPËRISË”

Në mbështetje të neneve 29, 30, 31 dhe 32 të ligjit nr. 9887, datë 10.03.2008 “*Për mbrojtjen e të dhënave personale*”, i ndryshuar (në vijim, “*Ligji*”), neneve 77-112 të 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 “*Banka e Bashkuar e Shqipërisë*” sh.a (në vijim “*Kontrolluesi/dhe ose UBA*”),

KONSTATOVA SE:

Në zbatim të Urdhrit nr. 188, datë 08.11.2024 të Komisionerit për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale (në vijim, “*Komisioneri*”), u krye hetim administrativ pranë Kontrolluesit me objekt:

- *Zbatimi i ligjit nr. 9887, datë 10.03.2008 “Për mbrojtjen e të dhënave personale”, i ndryshuar, me fokus masat tekniko-organizative për përpunimin e tyre, veçanërisht sistemet e menaxhimit të sigurisë së informacionit (SMSI).*

Komisioneri, pasi shqyrtoi relacionin e hetimit administrativ, procesverbalin e konstatimit dhe provat e administruara gjatë ushtrimit të hetimit pranë Kontrolluesit, vëren se:

1. Kontrolluesi “Banka e Bashkuar e Shqipërisë” është personi juridik i regjistruar në Regjistrin Tregtar Shqiptar me NIPT J91811004Q dhe ushtron veprimtari bankare dhe veprimtari të tjera tregtare të përcaktuara me rregullore nga Banka e Shqipërisë, sipas përcaktimeve të ligjit Nr. 9662, datë 18.12.2006 “*Për Bankat në Republikën e Shqipërisë*” dhe të ligjit Nr. 8269, datë 23.12.1997 “*Për Bankën e Shqipërisë*”.
2. Rezulton se, Kontrolluesi aplikon Formularin “Fleta teknike prezantuese” i cili mbledh të dhëna për kategoritë, “*Bashkëshorti(ja), Atësia, Mëmësia, Fëmijët dhe*

gjeneralitetet e tyre, Profesioni dhe punësimi aktual i bashkëshortit”, si dhe në dosjen e punonjësit administrohet, ndër të tjera, dokumenti “*Certifikatë familjare*”. Gjithashtu, rezulton se në regjistrin e vizitorëve Kontrolluesi, ndër të tjera, mbledh të dhëna si: “*Nr. pasaporte/ID*”.

Sa më sipër, konstatohet se këto të dhëna përpunohen në kundërshtim me parimin e mjaftueshmërisë sipas germës “c”, të pikës 1, të nenit 5 të Ligjit dhe 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 që të përpunojë ato të dhëna që ka të nevojshme për të arritur qëllimin duke respektuar parimin e mbrojtjes së të dhënave personale lidhur me mjaftueshmërinë e të dhënave, në të cilin parashikohet se mbledhja dhe përpunimi i të dhënave duhet të lidhet me qëllimin e përpunimit dhe të mos e tejkalojnë këtë qëllim.

3. Konstatohet se, Kontrolluesi ka të instaluar një sistem video-survejimi (CCTV) i cili mbikëqyr korridoret, ambientet e jashtme dhe ambientet e brendshme (të zyrave dhe njësive të tjera organizative), në kundërshtim me parashikimet e neneve 5 dhe 6 të Ligjit dhe Udhëzimit nr. 11.

Zyra e Komisionerit vlerëson se, një nga mjetet e rëndësishme të përpunimit të të dhënave personale është edhe sistemi i video/audio-survejimit (CCTV). Të dhënat e ruajtura në këto sisteme si “*imazhe*” dhe “*video*”, janë të dhëna personale, dhe përpunimi i tyre duhet të jetë në përputhje me parashikimet e Ligjit si dhe akteve të miratuara nga Komisioneri në lidhje me mbledhjen, përpunimin, ruajtjen dhe sigurinë e të dhënave personale, gjatë kryerjes së aktivitetit nga Kontrolluesit.

4. Kontrolluesi ka publikuar “*Politikat e Privatësisë*” në faqen e internetit <https://uba.com.al/>, megjithatë nga analizimi i saj rezulton se subjektet e të dhënave nuk informohen në gjuhën shqipe, për fushën dhe qëllimin, për të cilin do të përpunohen të dhënat personale, për mënyrën e përpunimit, të drejtën për akses, të drejtën për fshirje dhe/ose korrigjim të të dhënave, etj., në kundërshtim me parashikimet e nenit 18 të Ligjit.

Zyra e Komisionerit vlerëson se, informimi i subjekteve të të dhënave personale është i rëndësishëm, pasi u jep mundësinë subjekteve të të dhënave personale të njihen me të drejtat që gëzojnë, si dhe mundësinë e ushtrimit të tyre në praktikë. Mospërmbushja e këtij detyrimi nga Kontrolluesi mund të sjellë pasoja të rënda sa i përket privatësisë dhe përpunimit të të dhënave personale të subjekteve të të dhënave. Informimi sipas përcaktimeve të nenit 18 të Ligjit, duhet të aplikohet për çdo proces përpunimi të të dhënave personale të subjekteve të të dhënave, që kryen Kontrolluesi.

5. Veprimtaria e Kontrolluesit për përpunimin e të dhënave personale realizohet, ndër të tjera, nëpërmjet sistemeve elektronike Core Banking dhe Loan Origination.

Core Banking (përbëhet nga modulet për menaxhimin e llogarive, pagesat, kreditë, raportimin dhe përputhshmërinë) është infrastruktura kompjuterike ku bëhet përpunimi dhe ruajtja e të gjithë informacionit, mbi të gjithë shërbimet e ofruara në degët dhe filialet e Kontrolluesit. Mbi këtë infrastrukturë është i ngritur sistemi qendror për ofrimin e shërbimeve të informatizuar financiare, nëpërmjet të cilit ofrohet një numër i madh ndërfaqesh që mundësojnë lidhjen e sistemit qendror me njësitë e tjera organizative. Përdoruesit e këtij sistemi janë klientët, arkëtarët, oficerët e kredive dhe administratorët IT. Ky sistem centralizon dhe automatizon funksionet thelbësore bankare, duke bërë që shërbimet të jenë të aksesueshme në degë, ATM, platforma online dhe aplikacione mobile.

“Sistemi i menaxhimit të kredive” ose Loan Origination është një sistem i zhvilluar nga kompania Facilitation (Creatio) dhe shërben për të menaxhuar ciklin e dhënies së një kredie e cila kalon në disa faza të caktuara. Ky sistem aksesohet nga përdorues të bankës, sipas të drejtave të paracaktuara në funksionet e punës dhe ndahet në tre faza: *Contact* (krijimi i kontakteve për prospect customer ose customer), *Lead* (shprehje e interesit për kredi dhe analiza paraprake), si dhe *Application* (analiza e kredisë sipas procedurës së bankës).

Sistemet Core Banking dhe Loan Origination hostohen në makina virtuale dhe server fizik, me komponentë të ndryshëm mbështetës të teknologjisë së informacionit. Përdoruesit administrativ të sistemeve, operatorë/punonjës dhe klientët kanë mundësi që ti aksesojnë online. Site “Primar” dhe site “DRC”, janë të ngritura si makina virtuale dhe/ose fizike. Komponentët e infrastrukturës së rrjetit përfshijnë: Firewall, Hardware Servera, Switches, Storage Backup, etj.

Kontrolluesi disponon gjithashtu aplikacionin UBA Bank, i cili operon online për klientët, me qëllim marrjen e shërbimeve nga sistemet elektronike. Çdo përdorues që regjistrohet nëpërmjet këtij aplikacioni, plotëson të dhënat si, emri, mbiemri, adresa e email-it dhe numri i telefonit, etj. Adresa e email-it shërben në mënyrë që të merret kodi i aktivizimit. Aplikacioni UBA Bank, është një platformë digjitale e cila mundëson që nëpërmjet kompjuterit, smartphone-it ose tablet-it të kryhen veprimet e mëposhtme:

- Shkarkimi në mobile i aplikacionit dhe regjistrimi fillestar i përdoruesit;
- Kryerjen e veprimeve financiare dhe informuese;
- Ngarkim i gjendjes së llogarisë së klientit;
- Lidhja me profilin e klientit të shërbimeve të klientit;
- Kontrolli në kohë reale dhe në mënyrë të sigurt të të gjithë veprimeve financiare;
- Kontrollin e transfertave të parave në rolin e marrësit ose të dërguesit;
- Etj.

Nga verifikimi on-site i sistemeve elektronike dhe aplikacionit "UBA Bank" si dhe nga shqyrtimi i procedurave rregulluese që disponon Kontrolluesi, rezulton se:

- Nuk ka të specifikuar/dokumentuar kohën maksimale në të cilën shërbimet dhe sistemet nuk mund të jenë funksionale. Nuk janë planifikuar masa që në rast dështimi të një/disë pajisjeve të mos ndikohet në funksionimin e sistemeve dhe shërbimeve të ofruara;
- Nuk ka kryer auditim në lidhje me riskun dhe kontrollin e sigurisë së aplikacionit në të dy versionet e ofruara, Android dhe IOS;
- Nuk ka marrë masa për të kryer një vlerësim të ndikimit të operacioneve të përpunimit në të dhënat personale;
- Nuk ka procedura për testimin e protokolleve për sigurinë e aplikacioneve dhe shërbimeve online, veçanërisht për platformat "e-banking".

Për sa më sipër, Kontrolluesi nuk ka marrë masa organizative dhe teknike të përshtatshme për të mbrojtur të dhënat personale nga shkatërrime të paligjshme, aksidentale, humbje aksidentale, për të mbrojtur aksesin ose përhapjen nga persona të paautorizuar, veçanërisht në këtë rast kur përpunimi i të dhënave kryhet nëpërmjet komunikimeve elektronike, në kundërshtim me parashikimet e nenit 27 të Ligjit, si dhe 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*").

Zyra e Komisionerit vlerëson se, krijimi i procedurave dhe politikave të përdorimit të infrastrukturës TIK dhe sistemeve elektronike ku të specifikohet koha maksimale në të cilën shërbimet dhe sistemet janë funksionale dhe të disponueshëm, është një ndër masat kryesore që duhet të ndërmarrë Kontrolluesi, në lidhje me sigurinë dhe funksionimin e sistemeve të teknologjisë së informacionit.

Gjithashtu, Kontrolluesi duhet të kryejë auditime të vazhdueshme të sigurisë së informacionit gjatë përpunimit të tyre nëpërmjet sistemeve elektronike apo aplikacioneve. Gjetjet nga auditimet, duhet të adresohen dhe të analizohen në mënyrë periodike me qëllim parandalimin e çdo cedimi të mundshëm të funksionimit të sistemit apo integritetit të të dhënave që përpunohen nga përdorimi i aplikacioneve në të dy versionet e ofruara, Android dhe IOS.

Gjithashtu, vlerësimi i ndikimit të proceseve të përpunimit i jep mundësi Kontrolluesit që të analizojë rreziqet dhe masat mbrojtëse me qëllim rritjen e sigurisë së të dhënave personale.

Sa më sipër, Zyra e Komisionerit vlerëson se Kontrolluesi nuk ka marrë masa organizative dhe teknike të përshtatshme për të mbrojtur të dhënat personale nga shkatërrime të paligjshme, aksidentale, humbje aksidentale, për të mbrojtur aksesin ose përhapjen nga persona të paautorizuar, veçanërisht në këtë rast kur përpunimi i të

dhënave kryhet nëpërmjet komunikimeve elektronike, në kundërshtim me parashikimet e nenit 27 të Ligjit dhe Udhëzimit nr. 47, të Komisionerit.

6. Kontrolluesi ka lidhur “Kontratë Bashkëpunimi” me nr. 8099 prot., datë 12.02.2024 për sigurimin e jetës dhe shëndetit me shoqërinë e sigurimit “INSIG.JETE sh.a”.

Nga shqyrtimi i kontratës së sipërcituar, rezulton se në përmbajtje të saj nuk janë reflektuar detyrimet sipas parashikimeve në nenin 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 përdorimit e një kontrate tip në rastet e këtij delegimi*” i ndryshuar (në vijim “*Udhëzimi nr. 19*”).

Zyra e Komisionerit vlerëson se, në rastet e delegimit të përpunimit të të dhënave Kontrolluesi duhet të miratojë një akt/kontratë, që palët duhet të përdorin në rast të këtij delegimi, me anë të së cilës të garantojë përcaktimin e rregullave në marrëdhënien e tij me përpunuesin, me qëllim që delegimi i përpunimit të këtyre të dhënave të përpunuesit të jetë në përputhje me nenin 20 të Ligjit dhe me Udhëzimin nr. 19 të Komisionerit. Në rastet e delegimit të përpunimit të të dhënave dhe/ose shërbimit, Kontrolluesi duhet të sigurohet që përpunuesi të garantojë përpunim të ligjshëm dhe të sigurt të të dhënave.

7. Nga verifikimi i kryer në regjistrin elektronik të subjekteve kontrolluese, në protokollin e Zyrës së Komisionerit, rezulton se Kontrolluesi ka njoftuar mbi përpunimin e të dhënave personale për të cilat është përgjegjës. Nga analizimi i Formularit, është konstatuar se “*Njoftimi*” ka mangësi në deklaram, sa i përket rubrikave të formularit si vijon:

- Deklarimin në rubrikën 3.1, të formularit të njoftimit “*Kategoritë e subjekteve të të dhënave personale që përpunohen*” të tilla si “*vizitorë*”, etj.”;
- Deklarimi në rubrikën 4.1, të formularit të njoftimit “*Kategoritë e të dhënave personale që përpunohen*” të tilla si “*të dhëna të familjarëve*”, etj.”;

Konstatimet e mësipërme janë në kundërshtim me parashikimet e neneve 21 dhe 22 të Ligjit.

Zyra e Komisionerit vlerëson se realizimi i detyrimit për përditësimin e ndryshimit të gjendjes së njoftimit të përpunimit të të dhënave sipas parashikimeve të nenit 21 dhe 22 të Ligjit është i rëndësishëm, pasi i jep mundësinë subjekteve të të dhënave që të informohen mbi përpunimin që kryen Kontrolluesi dhe realizimin e detyrimeve ligjore. Kjo i jep mundësi reale subjektit të të dhënave për të ushtruar në mënyrë korrekte të drejtat që i jep Ligji.

8. Kontrolluesi disponon rregullore të brendshme, si dhe rregullore “*Për mbrojtjen, përpunimin, ruajtjen dhe sigurinë e të dhënave personale*”. Megjithatë, nga shqyrtimi i përmbajtjes së saj konstatohet se, rregullorja nuk përfshin në mënyrë të detajuar

proceset, procedurat, masat teknike dhe organizative specifike mbi mënyrën e përpunimit të të dhënave personale, sigurinë e të dhënave, konfidencialitetin, etj., në kundërshtim me parashikimet e nenit 27 të Ligjit.

Zyra e Komisionerit vlerëson se, është i nevojshëm rishikimi i këtij akti, ku të parashikohen rregulla dhe procedura organizative specifike mbi mënyrën e përpunimit të të dhënave personale, sigurinë e të dhënave, konfidencialitetin, sipas proceseve përpunuese gjatë kryerjes së aktivitetit nga Kontrolluesi, në përputhje me parashikimet e nenit 27 të Ligjit.

9. Kontrolluesi disponon një grup politikash të lidhur me sigurinë e informacionit, konkretisht:
 1. Politika e vëzhgimit me kamera;
 2. Procedurë mbi përpunimin e të dhënave personale mbi sistemin e video survejimit;
 3. Politikat e Privatësisë së UBA Bank;
 4. Rregullore mbi aksesin dhe sigurinë fizike në qendrat e të dhënave të teknologjisë së informacionit;
 5. Politika e menaxhimit të aktivëve informativ;
 6. Outsourcing procedure;
 7. Information security management system scope document;
 8. Information Security Statement of Applicability;
 9. Information Technology System Hardening Policy;
 10. Clean Desk Procedure;
 11. Information Security Policy.

Nga shqyrtimi i grupit të politikave konstatohet se, mungojnë dhe elementë të tjerë të sigurisë së të dhënave si, *“Analizën e Ndikimit në të Dhënat Personale”*, *“Raport vlerësimi mbi sigurinë në sistemin e arkivimit”*, si dhe *“Hapat që duhet të ndërmerren në rast incidentesh të shkeljes së sigurisë së të dhënave personale”*, etj., në kundërshtim me parashikimet e nenit 27 të Ligjit dhe Udhëzimit nr. 47.

Gjithashtu, nga verifikimi i përmbajtjes së manualit trajnues të punonjësve të Kontrolluesit rezulton se përmbajtja e tij nuk është e mjaftueshme, dhe ka nevojë të përfshijë të gjitha proceset përpunuese të Kontrolluesit, sipas parashikimeve të nenit 27 të Ligjit dhe sipas përcaktimeve në Kapitullin IV, të Udhëzimit nr. 47 të Komisionerit.

Për sa më sipër, Kontrolluesi nuk ka plotësuar detyrimet në lidhje me ngritjen, administrimin dhe mirëmbajtjen e sistemit të menaxhimit të sigurisë së informacionit (SMSI) lidhur me mbrojtjen e të dhënave personale, të parashikuara në Udhëzimin nr. 47 të Komisionerit, për shkak të cilësisë si subjekt përpunues i madh, si dhe për shkak të natyrës së veçantë të veprimtarisë që Kontrolluesi ushtron.

Zyra e Komisionerit vlerëson se, sipas parashikimeve të Kreut IV të Udhëzimit nr. 47, Kontrolluesi duhet të marrë masa konkrete në kuadër të trajnimit të punonjësve që kanë akses dhe përpunojnë të dhëna personale, bazuar në legjislationin në fuqi për mbrojtjen e të dhënave personale. Ky është një detyrim i vazhdueshëm i Kontrolluesit që personeli i subjektit përpunues të të dhënave personale të trajnohet rregullisht për mbrojtjen e të dhënave personale.

Gjithashtu, Zyra e Komisionerit vlerëson se, për shkak të cilësisë si subjekt përpunues i madh, si dhe për shkak të natyrës së veprimitarisë 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 në 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, “*Udhëzimit nr. 48*”) si dhe është një sistem i certifikueshëm, për qëllime përputhshmërie me standardin e sipërpërmendur, vetëm me organizma të akredituar dhe autorizuar sipas parashikimeve të Udhëzimit nr. 48.

Në përfundim të hetimit administrativ, referuar provave dhe konstatimeve në vend, grupi i inspektimit hartoi procesverbalin përkatës, një kopje e të cilit i është vendosur në dispozicion Kontrolluesit nëpërmjet rrugës postare.

Në respektim të së drejtës për t’u dëgjuar, në zbatim të neneve 87-89 të Kodit të Procedurave Administrative, Kontrolluesi është ftuar të marrë pjesë në seancë dëgjimore, përpara marrjes së vendimit përfundimtar nga ana e Komisionerit.

Përfaqësuesi i Kontrolluesit, gjatë seancës dëgjimore të zhvilluar, më datë 07.01.2025, ka parashtruar pretendimet me shkrim, si dhe ka depozituar dokumentacion plotësues mbi konstatimet e procesverbalit të hetimit administrativ, si vijon:

- Rregullore e Operimit, procedurat e administrimit të E/M Banking;
 - Procedure on Internet and Mobile Banking administration;
 - Rregullore mbi aksesin dhe sigurinë fizike në qendrat e të dhënave të teknologjisë së informacionit;
 - Marrëveshje ndërmjet UBA Bank dhe CLASTERTECH shpk me objekt: Testin e Penetritimit, sigurinë e sistemeve, testimin dhe vlerësimin e aksesit;
 - Technical Proposal;
 - Rregullore për mbrojtjen, përpunimin, ruajtjen dhe sigurinë e të dhënave personale.
- Lidhur me konstatimin në pikën 4 të Procesverbalit, Kontrolluesi pretendon se: “*Është proceduar menjëherë me publikimin në faqen e internetit të dokumentit “Politikat e Privatësisë” në gjuhën shqipe.*”

Zyra e Komisionerit vlerëson se, nga analizimi i përmbajtjes së rubrikës së politikave të privatësisë në faqen zyrtare të Kontrolluesit, informimi nuk është shterues në lidhje me qëllimin dhe mënyrën e përpunimit të të dhënave personale, personin që do t'i përpunojë të dhënat, të drejtat që subjektet e të dhënave gëzojnë (akses, korrigjim dhe fshirje) etj., në kundërshtim me parashikimet e nenit 18 të Ligjit.

Zyra e Komisionerit vlerëson se, informimi i subjekteve të të dhënave personale është një nga detyrimet bazë të Kontrolluesit, pasi u jep mundësinë subjekteve të të dhënave personale të njihen me të drejtat që gëzojnë dhe mundësinë e ushtrimit të tyre në praktikë. Mospërbushja e këtij detyrimi, nga ana e Kontrolluesit, mund të sjellë pasoja të rënda, sa i përket privatësisë dhe përpunimit të të dhënave personale të subjekteve të të dhënave.

Gjithashtu, Kontrolluesi argumentoi se “ *Do të merren të gjitha masat organizative për pozicionimin e kamerës për monitorim vetëm në funksion të qëllimit që është vendosur si dhe në zbatim të detyrimeve që rrjedhin nga Udhëzimi nr. 11, dhe jo vetëm. Gjithashtu Banka e Bashkuar e Shqipërisë do të përditësojë formularin e dërguar sipas të dhënave që përpunohen aktualisht nga banka, ndërkohë është proceduar menjëherë me publikimin në faqen e internetit të dokumentit “Politikat e Privatësisë” në gjuhën shqipe. Në përfundim, Banka e Bashkuar e Shqipërisë shpreh angazhimin maksimal në përmbushjen e vazhdueshme të kërkesave ligjore për mbrojtjen e të dhënave personale si dhe zbatimin e rekomandimeve të Komisionerit për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale”.*

Në përfundim, Zyra e Komisionerit vlerëson bashkëpunimin e Kontrolluesit me grupin e kontrollit, gjatë ushtrimit të hetimit administrativ, si 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 shmang mundësinë e përhapjes së tyre në mënyrë të paligjshme.

PËR KËTO ARSYE:

Në zbatim të neneve 5, 6, 18, 20, 21, 22, 27, 29, 30, 31 (pika 1, germa “a/1”), si dhe 32 të Ligjit,

REKOMANDOJ:

1. Kontrolluesi, të ketë në vëmendje përpunimin e të dhënave personale, në përputhje me dispozitat e parashikuara në Kreun II të Ligjit;
2. Kontrolluesi, në zbatim të nenit 5 të Ligjit, të marrë masa që mbledhja e të dhënave personale nga ana e tij, të kryhet në mënyrë të ligjshme, informacioni të grumbullohet vetëm për qëllime specifike, të përcaktuara qartë, e legjitime dhe përpunimi i të dhënave të kryhet në përputhje me këto qëllime, duke ju përmbajtur gjithashtu parimit

të mjaftueshmërisë së të dhënave, të cilat duhet të lidhen me qëllimin e përpunimit dhe të mos e tejkalojnë këtë qëllim;

3. Kontrolluesi, në zbatim të neneve 5 dhe 6 të Ligjit, të bëj një rivlerësim në lidhje me pozicionimin e kamerave dhe të ambienteve që do të mbikëqyren, në përputhje me qëllimin e përpunimit, duke vlerësuar ato raste në të cilat monitorimi përmes sistemit të kamerave tejkalon qëllimin;
4. Kontrolluesi, të marrë masa për zbatimin e detyrimeve, në lidhje me informimin e plotë të subjekteve të të dhënave, sipas parashikimeve të nenit 18 të Ligjit;
5. Kontrolluesi, të marrë masa për të rishikuar marrëveshjet e bashkëpunimit me përpunuesit duke specifikuar detyrimet midis palëve, sipas dispozitave të parashikuara në nenin 20 të Ligjit dhe Udhëzimin nr. 19 të Komisionerit;
6. Kontrolluesi, në zbatim të nenit 27 të Ligjit, të përfshijë në Rregulloren “*Për mbrojtjen, përpunimin, ruajtjen dhe sigurinë e të dhënave personale*”, masa konkrete teknike dhe organizative për mbrojtjen e të dhënave personale, mënyrën e përpunimit të të dhënave, të drejtat e subjekteve të të dhënave, garantimin e konfidencialitetit etj., në funksion të aktivitetit të tij, për çdo proces përpunimi;
7. Kontrolluesi, me qëllim garantimin e sigurisë së të dhënave personale duhet të zbatojë detyrimet e përcaktuara në Udhëzimin nr. 47, lidhur me trajnimin e punonjësve që kanë akses dhe përpunojnë të dhëna personale dhe krijimin, mirëmbajtjen dhe administrimin e Sistemit të Menaxhimit të Sigurisë së Informacionit (SMSI) për mbrojtjen e të dhënave personale;
8. Kontrolluesi, për shkak të natyrës së veçantë të aktivitetit që ushtron, duhet të marrë masat e nevojshme për të vlerësuar mbi certifikimin e sistemeve të menaxhimit të sigurisë së informacionit, të të dhënave personale dhe mbrojtjes së tyre, sipas parashikimeve të Udhëzimit nr. 48;
9. Në zbatim të pikës 1, të nenit 32 të Ligjit, të përmbushen detyrimet sipas këtij akti brenda afateve, si vijon:
 - (i) vazhdimisht, detyrimet e treguara në pikat 1 dhe 4 më sipër;
 - (ii) brenda 15 (pesëmbëdhjetë) ditëve, detyrimet e treguara në pikat 2 dhe 3 më sipër;
 - (iii) brenda 30 (tridhjetë) ditëve, detyrimet e përcaktuara në pikat 5 dhe 6 më sipër;
 - (iv) brenda 45 (dyzetë e pesë) ditëve, detyrimet e përcaktuara në pikën 7 më sipër.

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

10. Kontrolluesi të njoftojë Zyrën e Komisionerit për masat e marra;

11. Në rast mospërbushje të detyrimeve të parashikuara në këtë akt, Zyra e Komisionerit 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, Zyra e Komisionerit 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 30.01.2025.

KOMISIONERI

Besnik Dervishi