R E P U B L I K A E S H Q I P Ë R I S Ë
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. 838/10 prot. Tiranë, më 11.7.2025

REKOMANDIM

Nr.34, datë 11.7.2025

PËR KONTROLLUESIN "BANKA E TIRANËS"

Në mbështetje të neneve 81, 82, 83 dhe 84 të ligjit nr. 124/2024 "*Për mbrojtjen e të dhënave personale*", (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 Tiranës"*, Tiranë (në vijim *"Kontrolluesi"*),

KONSTATOVA SE:

Në zbatim të Urdhrit nr. 48, datë 05.03.2025 të Komisionerit për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale (në vijim,*"Komisioneri"*), u krye hetimi administrativ pranë Kontrolluesit me objekt:

- *Zbatim i ligjit nr. 124/2024 "Për mbrojtjen e të dhënave personale" dhe akteve të miratuara nga Komisioneri në lidhje me mbledhjen, përpunimin, ruajtjen dhe sigurinë e të dhënave personale, gjatë kryerjes së aktivitetit nga Kontrolluesi.*

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

1. Kontrolluesi është personi juridik i regjistruar në Regjistrin Tregtar Shqiptar me NIPT J61924008V dhe ushtron veprimtari bankare dhe veprimtari të tjera tregtare të përcaktuara me rregullore nga Banka e Shqipërisë, në Republikën 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*".

   Kontrolluesi përpunon të dhëna personale për kategoritë "*klientë*", "*punonjës*", "*furnizues*", "*vizitorë*", *etj*. Përpunimi i të dhënave kryhet në mënyrë manuale dhe elektronike.

2. Rezulton se, në regjistrin e vizitorëve, Kontrolluesi, ndër të tjera, mbledh të dhëna si; "*Nr. dokument identifikimi*".

   Sa më sipër, të dhënat për "*Nr. dokument identifikimi*" mblidhen dhe përpunohen, në kundërshtim me parimin e minimizimit, sipas pikës 3, të nenit 6 të Ligjit.

   Zyra e Komisionerit vlerëson se, Kontrolluesi ka detyrimin që të mbledhë dhe përpunojë të dhëna personale, në masën që ato janë të përshtatshme dhe të kufizuara në masën që është e nevojshme për realizimin e qëllimit, si dhe të mos e tejkalojnë këtë qëllim.

3. Kontrolluesi administron dokumentacionin për punonjësit aktual dhe punonjësit e larguar, në dosje fizike si dhe në mënyrë elektronike.

   Gjithashtu, rezulton se të dhënat personale të *"Klientëve të rastësishëm"* ruhen në sistemin elektronik Core Banking për një periudhë mbi 10 vite.

   Nga analizimi i dokumenteve të cilat parashikojnë procedurat dhe masat për proceset përpunuese, rezulton se Kontrolluesi nuk ka parashikuar afate konkrete lidhur me kohën e ruajtjes së të dhënave personale, për dokumentacionin që administron në funksion të veprimtarisë që ushtron.

   Sa më lart, të dhënat e mbledhura nga Kontrolluesi ruhen, pa përcaktuar një afat konkret të ruajtjes së tyre, në kundërshtim me pikën 5, të nenit 6 të Ligjit, si 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, lidhur me kategoritë e të dhënave të grumbulluara, në funksion të ushtrimit të veprimtarisë së tij, Kontrolluesi duhet të parashikojë mbajtjen e të dhënave personale të grumbulluara në atë formë, që lejon identifikimin për një kohë të caktuar, por jo më tepër se sa është e nevojshme për të përmbushur qëllimin për të cilin të dhënat janë grumbulluar. Koha e ruajtjes së të dhënave personale duhet të përcaktohet nga Kontrolluesi, në përputhje me parashikimin e pikës 5, të nenit 6 të Ligjit.

4. Kontrolluesi ka të instaluar sistemin e video survejimit CCTV, përmes të cilit kryen mbikëqyrjen e ambienteve ku ushtron veprimtarinë e tij si dhe të degëve në të gjithë territorin e vendit, me qëllim të mbrojtjes së pronës dhe sigurinë e kontrollit mbi hyrjet dhe daljet.

   Nga shqyrtimi i dokumentacionit "*Rregullore e Sigurisë fizike në degë*", të vendosur në dispozicion, rezulton se, lidhur me këtë proces përpunues, Kontrolluesi, në Rubrikën 7 "*Sistemi televiziv me qark të mbyllur CCTV, sistemi i vëzhgimit në degë*", pika 1, germa c, ka parashikuar afate për ruajtjen e imazheve, jo më pak se 15 ditë

dhe jo më shumë se 2 (dy) muaj. Nga verifikimi i sistemit të video survejimit CCTV konstatohet se, ato ruhen për një periudhë më të gjatë se 60 ditë, në kundërshtim me parimin e kufizimit të ruajtjes në kohë, sipas pikës 5, të nenit 6 të Ligjit dhe pikës 2, të nenit 3 të Udhëzimit nr. 3, datë 30.04.2025 të Komisionerit "*Për përpunimin e të dhënave personale nga sistemit e video survejimit*" (në vijim, "Udhëzimi nr. 3").

Zyra e Komisionerit vlerëson se, një nga mjetet e rëndësishme të përpunimit të të dhënave personale është edhe sistemi i video survejimit CCTV. Të dhënat e ruajtura në këto sisteme, si: "imazhe" e "video", janë të dhëna personale dhe përpunimi i tyre duhet të jetë në përputhje me parashikimet e Ligjit, si dhe aktet e miratuara nga Komisioneri në lidhje me mbledhjen, përpunimin, ruajtjen dhe sigurinë e të dhënave personale, gjatë kryerjes së aktivitetit nga Kontrolluesi.

Gjithashtu, Zyra e Komisionerit vlerëson se periudha e mbajtjes së të dhënave nuk duhet të kalojë kufirin maksimal të afatit të lejuar, për përmbushjen e qëllimit të video survejimit. Të dhënat e mbajtura me anë të sistemit të video survejimit duhet të ruhen për një periudhë të ligjshme të ruajtjes së regjistrimeve, e në momentin që qëllimi ka përfunduar duhet të realizojë shkatërrimin e të dhënave imazheve/video, në të kundërt përpunimi i mëtejshëm i të dhënave konsiderohet i paligjshëm, sipas parashikimeve të pikës 5, të nenit 6 të Ligjit dhe të Udhëzimit nr. 3 të Komisionerit.

5. Veprimtaria e Kontrolluesit për përpunimin e të dhënave personale realizohet, ndër të tjera, nëpërmjet sistemit elektronik Core Banking.

   Core Banking (përbëhet nga modulet për menaxhimin e llogarive, klientëve, transaksionet, kreditë, hipotekat, depozitave, investimeve, swift, kontrolli financiar, procesorët e kartave, raportimi, etj.) është infrastruktura kompjuterike ku kryhet përpunimi dhe ruajtja e të gjithë informacionit, mbi të gjithë shërbimet e ofruara në degët dhe filialet e shoqërisë.

   Mbi këtë infrastrukturë është i ngritur sistemi qendror i shoqërisë për ofrimin e shërbimeve të informatizuara financiare, ku nëpërmjet të cilit ofrohet një numër shumë i madh ndërfaqesh që mundësojnë lidhjen e sistemit qendror të shoqërisë me filialet në të gjithë vendin. 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 Core banking hostohet në makina virtuale dhe server-a fizik, me komponentë të ndryshëm mbështetës TIK. Përdoruesit administrativ të sistemeve, operatorë/punonjës dhe klientët, kanë mundësi që ti aksesojnë online shërbimet e ofruara nga ky sistem. Site "Primar" dhe site "DRC", janë të ngritura si makina virtuale dhe/ose fizike. Komponentët e infrastrukturës së rrjetit përfshijnë: Fireëall, Hardëare Servera, Sëitches, Storage Backup, etj.

Kontrolluesi disponon aplikacionin Tibank Mobile, 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, numri i telefonit, etj. Aplikacioni Tibank Mobile, është një platformë digjitale e cila mundëson që nëpërmjet kompjuterit, smartphone-it ose tablet-it të kryhen veprimet e mëposhtme:

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

Nga verifikimi on-site i sistemeve elektronike dhe aplikacionit "Tibank Mobile", si dhe nga shqyrtimi i procedurave rregulluese që disponon Kontrolluesi, konstatohet se:

- Nuk ka kryer audit në lidhje me riskun dhe kontrollin e sigurisë së aplikacionit "Tibank Mobile" 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 duke përdorur shërbimet mobile.

Në lidhje me verifikimet e mësipërme, Zyra e Komisionerit vlerëson se, 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 dhe integritetit të të dhënave që përpunohen nëpërmjet përdorimit të aplikacioneve në të dy versionet e ofruara, Android dhe IOS.

Mungesa e procedurave për testimin e protokolleve të sigurisë për aplikacionet dhe shërbimet online, veçanërisht për platformat e-banking, përbën një rrezik serioz në mbrojtjen e të dhënave personale, për arsyet se testimi i protokolleve ndihmon në zbulimin e dobësive të sigurisë, akseset e paautorizuara, rrjedhjet e të dhënave apo cenueshmëria ndaj sulmeve si man-in-the-middle.

Gjithashtu, Zyra e Komisionerit vlerëson se 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.

Për sa më sipër, rezulton se Kontrolluesi nuk ka marrë masa teknike e organizative, për të garantuar sigurinë e përpunimit të të dhënave personale që administron gjatë veprimtarisë, nga shkatërrime të paligjshme, 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 28 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*").

6. Kontrolluesi ka lidhur "*Marrëveshje Bashkëpunimi*", datë 01.12.2023 për sigurimin e punonjësve të kompanisë nga aksidentet, me shoqërinë e sigurimit "SIGAL UNIQA Group AUSTRIA" sh.a dhe "SIGAL Life UNIQA Group AUSTRIA" sh.a.

   Nga shqyrtimi i kontratës së sipërcituar, rezulton se në përmbajtje të saj nuk janë reflektuar detyrimet sipas parashikimeve në nenin 26 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 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 26 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 personale.

7. Kontrolluesi nuk disponon rregullore "*Për mbrojtjen e të dhënave personale*", ku të parashikohen proceset, procedurat, masat teknike dhe organizative sipas parashikimeve të nenit 28 të Ligjit, me qëllim garantimin e përpunimit të ligjshëm dhe sigurisë së të dhënave, në përputhje me proceset përpunuese të Kontrolluesit.

   Zyra e Komisionerit vlerëson se, hartimi i një rregulloreje "*Për mbrojtjen, përpunimin, ruajtjen dhe sigurinë e të dhënave personale*" përbën një detyrim thelbësor ligjor për çdo kontrollues, në zbatim të nenit 28 të Ligjit. Kjo rregullore duhet të përmbajë në mënyrë të detajuar rregulla dhe procedura mbi kategoritë e të dhënave personale që përpunohen, mënyrën e përpunimit, masat e sigurisë dhe konfidencialitetit, afatet e ruajtjes, të drejtat e subjekteve të të dhënave, si dhe përcaktimin e niveleve të aksesit, me qëllim garantimin e përpunimit të ligjshëm dhe sigurisë së të dhënave, në përputhje me proceset përpunuese të Kontrolluesit.

8. Kontrolluesi vendosi në dispozicion një grup politikash lidhur me sigurinë e informacionit, konkretisht:

1. Auditi i Brendshëm;
2. BCP TEST;
3. Kontrate kredie hipotekore;
4. Politikat e pasqyrimit;
5. Digital Marketing Procedure;
6. Digital onboarding;
7. G-Security;
8. Information Security Policies;
9. IS Procedures;
10. IT;
11. Recovery;
12. Risk Assessment;
13. Siguria Fizike;
14. Stafi;
15. Standard;
16. Risk Assessment pjesa e tretë;
17. Etj.

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 28 të Ligjit dhe Udhëzimit nr. 47 të Komisionerit.

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 28 të Ligjit dhe sipas përcaktimeve në Kapitullin IV, të Udhëzimit nr. 47 të Komisionerit.

Për sa më sipër, rezulton se, 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.

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 legjislacionin në fuqi për mbrojtjen e të dhënave personale.

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 legjislacionin 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 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 të Komisionerit.

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, "*Udhëzimi nr. 48*") si dhe është një sistem i certifikueshëm, për qëllime përputhshmërie me standardin e sipërpërmendur, vetëm me organizma të akreditуar 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.

Kontrolluesi, është paraqitur gjatë seancës dëgjimore të organizuar nga Zyra e Komisionerit, më datë 19.05.2025, dhe me shkresën nr. 10759 prot., datë 20.05.2025, administruar me tonën nr. 838/9 prot., datë 21.05.2025, parashtroi pretendime me shkrim, lidhur me konstatimet e grupit të kontrollit të Zyrës së Komisionerit si dhe ka depozituar në format CD, dokumentacion plotësues mbi konstatimet e procesverbalit të hetimit administrativ, si vijon:

- Rregullore e Sigurisë në Degë, V6/2024;
- Evidenca dhe pamje nga sistemi i bankës për ditët e regjsitirmit në degë;
- Kuadri rregullator në fuqi të Bankës për përputhshmërinë me Mbrojtjen e të Dhënave Personale;
- Qarkore nr. 190, "Planifikimi i masave për zbatimin e Ligjit nr. 124/2024 "Për mbrojtjen e të Dhënave Personale";
- Materialet e trajnimeve të personelit të bankës dhe testimet respektive për njohuritë në lidhje me Mbrojtjen e të Dhënave Personale.

- Lidhur me konstatimin në pikën 2 të Procesverbalit, Kontrolluesi pretendon se: "*Banka është një institucion i rëndësishëm dhe veprimet e punonjësit të recepsionit rregullohen me procedura të miratuara dhe bazohen në parimet më të mira të sigurisë. Informacioni i marrë është i minimizuar (emër, mbiemër, numër dokument identifikimi) dhe vetëm në funksion* të *sigurisë në zyrat qendrore. Ky proces kryhet për rritjen e sigurisë në zyrat qendrore dhe identifikimin e personave (jo staf i zyrave qendrore) që hyjnë në këto ambiente. Të dhënat e regjistruara nuk vendosen/ruhen në asnjë sistem dhe as nuk përpunohen më tej. Ato aksesohen vetëm në rast pajisje me kartë vizitori, nuk i regjistrohet numër dokument identifikimi.".*

  Zyra e Komisionerit vlerëson se, të dhënat personale të mbledhura nga Kontrolluesi në regjistrin e vizitorëve duhet të përpunohen vetëm në masën (sipas parimit të minimizimit) që janë të përshtatshme, të nevojshme dhe të mjaftueshme për realizimin e qëllimit të përpunimit, pa e tejkaluar këtë qëllim.

- Lidhur me konstatimin në pikën 7 të Procesverbalit, Kontrolluesi pretendon se: "*Banka ka një kuadër rregullator të vënë në dispozicon edhe Komisionerit, përmes të cilit mbështet përputhshmërinë me DP, i cili përbëhet nga:*
  - *Politika e Përputhshmërisë e Tirana Bank;*
  - *Politika e Mbrojtjes së të Dhënave Personale;*
  - *Politika e Privatësisë së të Dhënave Personale;*
  - *Procedura e Menaxhimit të të Drejtave të Subjektit të të Dhënave;*
  - *Korniza rregullatore dhe Metodologjia për Vlerësimin e Ndikimit në Mbrojtjen e të Dhënave Personale;*
  - *Regjistrimi i aktiviteteve të përpunimit- hartografia e të dhënave personale;*
  - *Politikat e Sigurisë së Informacionit;*
  - *Procedurat dhe Metodologjitë e Sigurisë së Informacionit;*
  - *Vlerësimi i Sigurisë së Sistemeve;*
  - *Rishikimi i Akseseve dhe profileve të punonjësve në sisteme;*
  - *Raporti i Vlerësimit të Rrezikut të Sigurisë së Informacionit;*
  - *Vlerësimi i Rrezikut për palë të treta;*
  - *Raporti i Analizës së Impaktit të Biznesit;*
  - *Raportet e testimeve të Planit të Vazhdimësisë së Biznesit;*
  - *Trajnimet e Sigurisë së Informacionit për punonjësit e Bankës dhe emaile ndërgjegjësuese;*
  - *Monitorimi i KRI-ve të Departamentit të Sigurisë së Informacionit;*
  - *Raport mbi Infrastrukturën e Sigurisë së Informacionit;*
  - *Inventari i aplikacioneve.*

  Lidhur me këtë pretendim, Zyra e Komisionerit vlerëson se hartimi i një rregulloreje "*Për mbrojtjen, përpunimin, ruajtjen dhe sigurinë e të dhënave personale*" përbën një detyrim thelbësor ligjor për çdo kontrollues, në zbatim të nenit 28 të Ligjit. Kjo rregullore duhet të përmbajë në mënyrë të detajuar rregulla dhe procedura mbi kategoritë e të dhënave personale që përpunohen, mënyrën e përpunimit, masat e sigurisë dhe konfidencialitetit, afatet e ruajtjes, të drejtat e subjekteve të të dhënave,

si dhe përcaktimin e niveleve të aksesit, me qëllim garantimin e përpunimit të ligjshëm dhe sigurisë së të dhënave, në përputhje me proceset përpunuese të kontrolluesit.

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 6, 26, 28, 81, 82, 83 dhe 84 të Ligjit,

REKOMANDOJ:

1. Kontrolluesi, të ketë në vëmendje proceset e përpunimit të të dhënave personale, në mënyrë që përpunimi mos të jetë në tejkalim të parimit të minimizimit të të dhënave, në përputhje me parashikimin e pikës 3, të nenit 6, të Ligjit;

2. Kontrolluesi të marrë masa për të shkatërruar në mënyrë të parikuperueshme të dhënat "video" të mbledhura për subjektet e të dhënave, të cilat janë përpunuar nëpërmjet sistemit CCTV, në përputhje me parashikimet ne nenit 6 të Ligjit dhe Udhëzimin nr. 3 të Komisionerit. Në këtë kuadër, të mbajë evidenca për shkatërrimin;

3. Kontrolluesi, të marrë masa për të rishikuar marrëveshjet e bashkëpunimit me përpunuesit duke specifikuar detyrimet midis palëve, sipas dispozitave të parashikuara në nenin 26 të Ligjit dhe Udhëzimin nr. 19 të Komisionerit;

4. Kontrolluesi, në zbatim të nenit 28 të Ligjit, të hartojë rregulloren "*Për mbrojtjen, përpunimin, ruajtjen dhe sigurinë e të dhënave personale*", duke parashikuar në të, masa konkrete teknike dhe organizative për mbrojtjen e të dhënave personale, për çdo kategori të dhënash dhe për çdo proces përpunimi, mënyrat e përpunimit të të dhënave, të drejtat e subjekteve të të dhënave, etj.;

5. 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;

6. 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 të Komisionerit;

7. Në zbatim të nenit 84 të Ligjit, të përmbushen detyrimet sipas këtij akti brenda afateve, si vijon:

(i) menjëherë, detyrimin e përcaktuar në pikën 2 më sipër;
(ii) vazhdimisht, detyrimet e treguara në pikën 1 më sipër;
(iii) brenda 30 (tridhjetë) ditëve, detyrimet e përcaktuara në pikat 3 dhe 4 më sipër;
(iv) brenda 45 (dyzetë e pesë) ditëve, detyrimet e përcaktuara në pikat 5 dhe 6 më sipër;

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

8. Kontrolluesi të njoftojë Komisionerin për masat e marra;

9. Në rast mospërmbushje të detyrimeve të parashikuara në këtë akt, Komisioneri, bazuar në germën "a", pika 2, e nenit 83 të Ligjit, paralajmëron kontrolluesit ose përpunuesit se veprimet e përpunimit mund të rezultojnë në mosplotësim të dispozitave ligjore dhe u jep atyre rekomandime lidhur me përputhshmërinë me ligjin. Në rast shkeljesh serioze ose të qëllimshme të dispozitave ligjore, Komisioneri vepron sipas neneve 92, 93 dhe 94 të Ligjit, për vendosjen e sanksioneve administrative në përputhje me nenet përkatëse, si dhe në përputhje me legjislacionin në fuqi për kundërvajtjet administrative, në mënyrë të tillë që këto masa të jenë efektive, proporcionale dhe me karakter parandalues.

Ky Rekomandim u shpall sot, më 11.7.2025.

KOMISIONERI

Besnik Dervishi