



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. 2110 prot.

Tiranë, më 26.12.2024

VENDIM

Nr. 43, datë 26.12.2024

PËR KONTROLLUESIN “INFORMATION BUSINESS SYSTEMS - IBS” SHPK

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 “Information Business Systems - IBS” shpk (në vijim “Kontrolluesi ose IBS”),

KONSTATOVA SE:

Në zbatim të Urdhrit nr. 151, datë 27.09.2024 të Komisionerit për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale (në vijim “Komisioneri”), u krye hetimi 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 grupit të hetimit, procesverbalin e hetimit administrativ dhe provat e administruara gjatë ushtrimit të hetimit pranë Kontrolluesit, vëren se:

1. IBS është një shoqëri e regjistruar me numër identifikimi J61820057C në Tiranë i cili ka si objekt të aktivitetit të tij, ndër të tjera, dhe tregtim i pajisjeve elektronike, sisteme access control, sisteme të biletarive elektronike, sisteme anti-zjarr, sisteme të parkimit qytetas dhe ndërqytetas, sisteme video konference audiovizive, mirëmbajtje dhe konsulencë software, hostim i faqeve web, zhvillim dhe mirëmbajtje i rrjetave të komunikimit network dhe telefonisë etj.

IBS përpunon të dhëna personale për kategoritë “*klientë*”, “*punëmarrës*”, “*furnizues*”, etj. Përpunimi i të dhënave kryhet në mënyrë manuale dhe elektronike.

2. Konstatohet se, Kontrolluesi nuk ka të publikuar “*Politikat e Privatësisë*” në faqen e internetit <https://www.ibs.al/>. Subjektet e të dhënave nuk informohen mbi qëllimin dhe mënyrën e përpunimit të të dhënave personale, personin që do t’i përpunojë të dhënat, afatin e mbajtjes së të dhënave, masat e sigurisë, të drejtat që subjektet e të dhënave gëzojnë (për akses, korrigjim dhe fshirje), etj, në kundërshtim me parashikimet e nenit 18 të Ligjit.

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.

3. Nga verifikimi i kryer në regjistrin elektronik të subjekteve kontrolluese dhe në protokollin e Zyrës së Komisionerit rezulton se, IBS nuk ka “*Njoftuar*” mbi përpunimin e të dhënave personale për të cilat është përgjegjës, në kundërshtim me parashikimet e nenit 21 dhe 22 të Ligjit.

Në datë 07.11.2024, pas marrjes në dijeni të urdhrit të hetimit administrativ, IBS ka depozituar nëpërmjet postës elektronike, formularin e “*Njoftimit*” mbi përpunimin e të dhënave personale për të cilat është përgjegjës.

Megjithatë, konstatohet se “*Njoftimi*” ka mangësi në deklarin, sa i përket rubrikave të formularit, si vijon:

- i. Deklarimin në rubrikën 3, të formularit të njoftimit “*kategoritë e subjekteve të të dhënave personale që përpunohen*”, të tilla si: “*nëpunës*” etj.;
- ii. Deklarimin në rubrikën 4, të formularit të njoftimit “*kategoritë e të dhënave personale që përpunohen*”, të tilla si: “*të dhënat e identifikimit*”, “*adresa*”, etj;
- iii. Deklarimin në rubrikën 6.1, të formularit të njoftimit “*qëllimi i përpunimit*”, të tilla si: “*menaxhim i burimeve njerëzore*”.

Zyra e Komisionerit vlerëson se, detyrimi për “*Njoftim*” mbi përpunimin e të dhënave personale, për të cilat Kontrolluesi është përgjegjës, sikurse edhe përditësimet e vazhdueshme të gjendjes së përpunimit, është i rëndësishëm, pasi i jep mundësinë subjekteve të të dhënave që të informohen për përpunimin e të dhënave të tyre, nga ana e Kontrolluesit, si dhe në realizimin e detyrimeve ligjore

të këtij të fundit. Kjo i jep mundësi reale subjekteve të të dhënave për të ushtruar të drejtat e tyre, sipas Ligjit.

4. IBS nuk ka hartuar rregullore “*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., por edhe akteve të tjera të brendshme të cilat parashikojnë masa teknike dhe organizative për procese të ndryshme përpunuese, në kundërshtim me nenin 27 të Ligjit, pasi shmang pasojat e rënda që mund të vijnë për subjektet e të dhënave personale.

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 teknike-organizative mbi mënyrën e përpunimit të të dhënave personale, (për çdo kategori subjektësh), 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, duke mundësuar shmangien e pasojave të rënda që mund të vijnë për subjektet e të dhënave.

5. IBS ka vendosur në dispozicion të grupit të kontrollit një certifikatë të standardit ndërkombëtar për menaxhimin e sigurisë së informacionit (Information Security Management System - ISMS), për krijimin, implementimin, mirëmbajtjen dhe përmirësimin e vazhdueshëm të një sistemi menaxhimi të sigurisë së informacionit, për menaxhimin e informacionit dhe mbrojtjen nga kërcënimet.

Megjithatë, nga analizimi i përmbajtjes së dokumentacionit rezulton se, në raport me proceset përpunuese që ushtron gjatë aktivitetit, sipas standardit ndërkombëtar për menaxhimin e sigurisë së informacionit, Kontrolluesi nuk disponon politika/procedura apo akte rregullatorë që janë dokumente shoqëruese, të tilla si: “Politikat e Sigurisë së Informacionit”, “Politikat e Menaxhimit të Incidenteve të Sigurisë”, “Regjistrat e gjurmimit të brendshëm dhe gjetjet”, “Analiza e Riskut në të dhënat personale”, Vlerësimi i Riskut”, etj.

Gjithashtu, rezulton se, mungojnë elementë të tjerë të sigurisë së të dhënave si: “Analizën e Ndikimit në të Dhënat Personale”, “Politikat e Sigurisë së Informacionit”, “Analiza e sigurisë së sistemit të arkivimit”, “Raport vlerësimi mbi sigurinë në sistemin e arkivimit”, “Sigurinë e personelit dhe pajisjeve elektronike të lëvizshme ose jo”, si dhe “Hapat që duhet të ndërmerren në rast incidentesh të shkeljes së sigurisë së të dhënave personale”, në kundërshtim me parashikimet e nenit 27 të Ligjit, Vendimin nr. 6, datë 05.08.2013 të Komisionerit “*Për përcaktimin e rregullave të hollësishme për sigurimin e të dhënave personale*” (në vijim “*Vendimi nr. 6*”) 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”).

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.

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 aktet rregullatore dhe politikat e lartpërmendura, si dhe të 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.

6. IBS nuk ka ndërmarrë masa konkrete në kuadër të trajnimit të punonjësve që kanë akses dhe përpunojnë të dhëna personale, lidhur me legjislacionin shqiptar në fuqi për mbrojtjen e të dhënave personale, sipas parashikimeve të Kreut IV, të Udhëzimit nr. 47.

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.

7. IBS nuk aplikon për punëmarrësit “*Deklaratën e Konfidencialitetit*”, në kundërshtim me nenin 28 të Ligjit.

Zyra e Komisionerit vlerëson se, qëllimi i nënshkrimit të “*Deklaratës së Konfidencialitetit*” është që të gjithë punonjësit, të cilët kanë akses në të dhënat personale, të kuptojnë qartë dhe drejtë, detyrimet dhe përgjegjësitë që ata kanë mbi përpunimin e të dhënave personale dhe ruajtjen e konfidencialitetit.

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 më datë 21.11.2024, paraqiti pretendimet me shkrim mbi konstatimet e procesverbalit, protokolluar me nr. 2110/5 prot.

- Lidhur me konstatimin e pikës 2 të Procesverbalit, për publikimin e *“Politikave të Privatësisë”*, në faqen zyrtare të Kontrolluesit, ky i fundit, pretendon se nuk ka publikuar politikat e privatësisë në website, pasi nuk mbledh dhe nuk përpunon të dhëna personale, si dhe nuk administron të dhëna sensitive, sipas nenit 18 të Ligjit.”

Zyra e Komisionerit vlerëson, se IBS përpunon të dhëna personale të klientëve, vizitorëve, punonjësve dhe si i tillë gëzon cilësinë e Kontrolluesit. Gjithashtu, çdo kontrollues që përpunon të dhëna personale, pavarësisht faktit nëse përpunimi bëhet në mënyrë elektronike apo manuale, dhe pavarësisht faktit nëse mbledh apo jo të dhëna personale nëpërmjet faqes zyrtare të internetit, ka detyrim që të publikojë *“Politikat e Privatësisë”*, me qëllim që të informojë qartësisht subjektet e të dhënave, pasi kontakti paraprak i çdo subjekti të dhënash me kontrolluesin realizohet nëpërmjet faqes së internetit.

- Lidhur me konstatimin në pikën 4 të Procesverbalit, se nuk është hartuar një *“Rregullore për mbrojtjen, përpunimin, ruajtjen dhe sigurinë e të dhënave personale”*, kontrolluesi pretendon se një rregullore e tillë është hartuar dhe dërguar grupit të inspektimit përmes postës elektronike.

Në lidhje me këtë pretendim, Zyra e Komisionerit vlerëson se, dokumenti i dërguar me postë elektronike, në datë 14.10.2024 (pas fillimit të hetimit administrativ) nga Kontrolluesi me emërtimin *“Rregullore e Brendshme”* nuk ka të parashikuara në përmbajtjen e saj dispozita për proceset, procedurat, masat tekniko-organizative specifike mbi mënyrën e përpunimit të të dhënave personale, sigurinë e të dhënave, konfidencialitetin, afatet e mbajtjes së të dhënave, etj., lidhur me veprimtarinë e Kontrolluesit, në kundërshtim kjo me parashikimet e nenit 27 të Ligjit. Në përmbajtje të saj kjo rregullore përmban rregullime të përgjithshme lidhur me etikën gjatë orarit të punës dhe jo masa konkrete për të dhënat personale dhe përpunimin e tyre gjatë veprimtarisë së Kontrolluesit.

- Lidhur me konstatimin në pikën 7 të Procesverbalit, se IBS nuk aplikon *“Deklaratën e konfidencialitetit”* për punëmarrësit, Kontrolluesi pretendon se: *“Konfidencialiteti”*

është i parashikuar si dispozitë e veçantë në Kontratën e punës së secilit prej punëmarrësve”.

Në lidhje me këtë pretendim, Zyra e Komisionerit, vlerëson se nuk qëndron, pasi aplikimi dhe nënshkrimi i “*Deklaratës së Konfidencialitetit*”, është i rëndësishëm që të gjithë punonjësit të cilët kanë akses në të dhënat personale, të kuptojnë qartë dhe drejtë, detyrimet dhe përgjegjësitë që ata kanë mbi përpunimin e të dhënave personale dhe ruajtjen e konfidencialitetit.

Në përfundim, shkeljet e konstatuara gjatë ushtrimit të hetimit administrativ, në kuptim të germave “*b*”, “*d*” dhe “*dh*”, të pikës 1, të nenit 39 të Ligjit, përbëjnë kundërvajtje administrative dhe sanksionohen me gjobë, si më poshtë:

- b) kontrolluesit, që nuk përmbushin detyrimin për të informuar, të përcaktuar në nenin 18 të këtij ligji, dënohen me 10 000 deri në 300 000 lekë;*
- d) kontrolluesit, që nuk përmbushin detyrimin për të njoftuar, sipas përcaktimit në nenin 21 të këtij ligji, dënohen me 10 000 deri në 500 000 lekë;*
- dh) kontrolluesit ose përpunuesit, që nuk marrin masat e sigurisë së të dhënave dhe nuk zbatojnë detyrimin për ruajtjen e konfidencialitetit, të përcaktuara përkatësisht në nenet 27 dhe 28 të këtij ligji, dënohen me nga 10 000 deri në 150 000 lekë;*

Në bazë të pikës 2, të nenit 39 të Ligjit, personat juridikë, për kundërvajtjet e mësipërme administrative, dënohen me dyfishin e gjobës së përcaktuar në pikën 1 të këtij neni.

Për zgjedhjen e masës së gjobës, Zyra e Komisionerit ka parasysh faktin se shkeljet e konstatuara janë serioze. Ato lidhen me garantimin e parimeve dhe përpunimin e ligjshëm të të dhënave, me informimin dhe garantimin e të drejtave të subjekteve të të dhënave, si dhe marrjen e masave të përshtatshme tekniko-organizative për sigurinë e të dhënave personale. Gjithashtu, vendimi i Komisionerit bazohet në mënyrën e reagimit të Kontrolluesit për rikuperimin e shkeljeve të konstatuara.

PËR KËTO ARSYE:

Në zbatim të neneve 18, 21, 22, 27, 28, 29, 30, 39 pika 1, germa “*b*”, “*d*” dhe “*dh*”, si dhe nenet 40 dhe 41 të Ligjit,

V E N D O S A:

- 1-** Dënimin e Kontrolluesit me gjobë në vlerën 40 000 (dyzet mijë) lekë, për shkelje të detyrimit të përcaktuar në nenin 18 të Ligjit;
- 2-** Dënimin e Kontrolluesit me gjobë në vlerën 20 000 (njëzet mijë) lekë, për shkelje të detyrimit të përcaktuar në nenin 21 të Ligjit;

- 3- Dënimin e Kontrolluesit me gjobë në vlerën 60 000 (gjashtëdhjetë mijë) lekë, për shkelje të detyrimit të përcaktuar në nenin 27 të Ligjit;
- 4- Kontrolluesi, të marrë masa konkrete, për përmbushjen e detyrimit për informimin e subjekteve të të dhënave personale, në gjuhën shqipe, përmes publikimit të politikave së privatësisë në faqen e internetit, në zbatim të detyrimeve të nenit 18 të Ligjit;
- 5- Kontrolluesi, në zbatim të neneve 21 dhe 22 të Ligjit, të ketë në vëmendje përditësimin e “Njoftimit” në lidhje me ndryshimin e gjendjes së njoftimit të përpunimit të të dhënave personale, për të cilat është përgjegjës;
- 6- Kontrolluesi, në zbatim të nenit 27 të Ligjit, të marrë masa për hartimin e rregullores “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, mënyrat 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, të zbatojë detyrimet e përcaktuara në Udhëzimin nr. 47, sa i përket krijimit, mirëmbajtjes dhe administrimit të 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 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;
- 9- Në zbatim të pikës 1, të nenit 32 të Ligjit, të përmbushen detyrimet, sipas këtij akti brenda afateve, si vijon:
 - i. brenda 15 (pesëmbëdhjetë) ditëve, detyrimet e treguara në pikat 4 dhe 5 më sipër.
 - ii. brenda 30 (tridhjetë) ditëve, detyrimet e treguara në pikën 6 më sipër.
 - iii. brenda 45 (dyzetë e pesë) ditëve, detyrimin e treguar në pikat 7 dhe 8 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- Gjoha arkëtohet nga kundërvajtësi në Buxhetin e Shtetit, jo më vonë se 30 (tridhjetë) ditë nga komunikimi i këtij Vendimi. Me kalimin e këtij afati, ky Vendim kthehet në titull ekzekutiv dhe ekzekutohet në mënyrë të detyrueshme nga Zyra e Përmbartimit;

12- Kundër këtij Vendimi mund të bëhet ankim në Gjykatën Administrative të Shkallës së Parë Tiranë, brenda 30 (tridhjetë) ditëve nga komunikimi i këtij Vendimi.

Ky Vendim u shpall sot, më datë 26.12.2024.

KOMISIONERI

Besnik Dervishi