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. 2107/7 prot. Tiranë, më 26.12.2024

VENDIM

Nr. 42, datë 26.12.2024

PËR KONTROLLUESIN "SINTEZA & CO" 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 *"Sinteza & CO" Shpk* (në vijim, *"Kontrolluesi"*),

KONSTATOVA SE:

Në zbatim të Urdhrit nr. 148, 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:

- *"Zbatim 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 është një shoqëri e regjistruar me numër identifikimi K11324003F, në Tiranë, i cili ka si objekt të aktivitetit të tij, ndër të tjera, dhe projektim / instalim rrjetesh kompjuterike / elektrike / telekomunikacioni, sisteme printimi, sisteme menaxhimi të dokumenteve, sigurisë kibernetike, server-room, zhvillim dhe implementim software, etj.

Adresa: Rruga *"Abdi Toptani"*, Nd.5, Tiranë Telefon: +355 42237200 www.idp.al, info@idp.al

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

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

   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.

   Të dhënat e mbledhura nga Kontrolluesi ruhen, pa përcaktuar një afat konkret të ruajtjes së tyre, në kundërshtim me germën *"d"* të pikës 1, të nenin 5 të Ligjit, si dhe me Udhëzimin nr. 11, datë 08.09.2011 të Komisionerit "*Mbi 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, në përputhje me parashikimin e germës "*d*", të pikës 1, të nenit 5 të Ligjit.

3. Kontrolluesi disponon një sistem të video-survejimit (CCTV) për mbikëqyrjen e ambienteve të jashtme. Nga verifikimi i kryer në vend konstatohet se, Kontrolluesi nuk disponon tabelë informimi për mbikëqyrjen e ambjenteve me sistemin CCTV, në kundërshtim me parashikimin e nenit 18 të Ligjit dhe Udhëzimin nr. 3, datë 05.03.2010 të Komisionerit "*Mbi përpunimin e të dhënave personale me sistemin e video-survejimit në ndërtesa dhe mjedise të tjera*", i ndryshuar (në vijim, "*Udhëzimi nr. 3*").

   Informimi i subjekteve të të dhënave personale mbi prezencën e sistemit të video-survejimit (CCTV) është një nga detyrimet bazë të Kontrolluesit. Sipas Udhëzimit nr. 3, subjektet e të dhënave duhet të informohen qartësisht që një sistem video-survejimi është në veprim, duke vendosur në ambientet e survejuara modelin standard të tabelës informuese për mbikëqyrjen me sistemin e survejimit, të miratuar nga Komisioneri.

4. Kontrolluesi disponon faqen web "https://sinteza-al.com/". Konstatohet se, Kontrolluesi nuk ka të publikuar rubrikën *"Privacy Policy/Politikat e Privatësisë".*

   Subjektet e të dhënave personale nuk informohen mbi qëllimin dhe mënyrën e përpunimit të të dhënave personale, personin që do t'i përpunojë të dhënat, të drejtat

Adresa: Rruga *"Abdi Toptani"*, Nd.5, Tiranë Telefon: +355 42237200 www.idp.al, info@idp.al

ligjore që gëzojnë, afatin e mbajtjes së të dhënave, dhe masat e sigurisë, 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. Kontrolluesi ka lidhur Kontratë Shërbimi Mirëmbajtje me palë të treta, të tilla si "Infosoft SD SHPK", me objekt *"...ofrimi i shërbimeve të mirëmbajtjes mbi sistemet kompjuterike...*".

   Nga analizimi i kontratës rezulton se, në pikën 5 "*Shërbimet e ofruara*" është parashikuar se Sipërmarrësi (Infosoft SD SHPK) kryen shërbime për Klientin (Sinteza Co SHPK):... 5.2) sipas kërkesës së Klientit për eliminimin e defekteve në S.K.I (rikuperim i informacionit në mbartësit informatik) dhe rivënien në punë. Këtu dallohen elementet si "*Punë Specialisti*" dhe "*Rregullimi/ Rikuperimi i të dhënave të dëmtuara*".

   Për sa më sipër, grupi i hetimit konstaton se, në përmbajtje të Kontratës nuk janë reflektuar detyrimet sipas parashikimeve në nenin 20 të Ligjit dhe Udhëzimit nr. 19 të Komisionerit, datë 03.08.2012 "*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 miratoj një 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 jetë në përputhje me nenin 20 të Ligjit dhe me Udhëzimin nr. 19 të Komisionerit.

6. Nga verifikimi i kryer në regjistrin elektronik të subjekteve kontrolluese dhe në protokollin e Zyrës së Komisionerit rezulton se, Kontrolluesi nuk ka "*Njoftuar*" mbi përpunimin e të dhënave personale për të cilat është përgjegjës në kundërshtim me parashikimin e nenit 21 të Ligjit.

   Në datë 8.10.2024 (pas fillimit të hetimit administrativ) nëpërmjet email-it, ka dorëzuar Formularin e Njoftimit.

   Zyra e Komisionerit vlerëson se, detyrimi për *"Njoftim"* mbi përpunimin e të dhënave personale, sikurse edhe përditësimet e vazhdueshme të gjendjes së përpunimit, sipas

Adresa: Rruga *"Abdi Toptani"*, Nd.5, Tiranë Telefon: +355 42237200 www.idp.al, info@idp.al

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, si dhe për realizimin e detyrimeve ligjore. Kjo i jep mundësi reale subjekteve të të dhënave për të ushtruar të drejtat e tyre që i jep Ligji.

7. Kontrolluesi vendosi në dispozicion një grup politikash të miratuara dhe të pa miratuara (*draft*) në gjuhën jo shqip lidhur me sigurinë e informacionit, konkretisht:

- Data protecion policy;
- Cyber Protection Plan;
- Asset management policies (Work in progress 95 % Completet);
- Cyber incident response plan (80% completed);
  - Anex 2 – cyber incident Response phishing playbook
  - Anex 3 – cyber incident Response data breach playbook;
  - Anex 4 – cyber incident Response malware playbook;
  - Anex 5 – cyber incident Response ransomware playbook;
  - Anex 6 – cyber incident Response redenial of service playbook;
- ISO 27001 2022 & GDPR Roles & Responsibilities (Final Draft):
- Backup and recovery policy (90% completed);
- GDPR DPIA Assessment;
- Access controll policy;
- Vulnerability and patch management policy;
- Network security policy;
- Gap Analysis Entry Meeting;
- Gap analysis process & data protection compliance.

Nga shqyrtimi i grupit të politikave konstatohet se, mungojnë dhe elementë të tjerë të sigurisë së të dhënave si, "Analiza e sigurisë së sistemit të arkivimit", "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", në kundërshtim me parashikimet e nenit 27 të Ligjit 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*").

Gjithashtu, Kontrolluesi 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.

Zyra e Komisionerit vlerëson se, 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 si dhe në zbatim të Udhëzimit nr. 47 të Komisionerit.

Adresa: Rruga *"Abdi Toptani"*, Nd.5, Tiranë Telefon: +355 42237200 www.idp.al, info@idp.al

Për sa më sipër, kontrolluesi nuk ka plotësuar detyrimet në lidhje 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, 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 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 akreditуar dhe autorizuar sipas parashikimeve të Udhëzimit nr. 48.

8. Kontrolluesi nuk aplikon për punëmarrësit "*Deklaratën e Konfidencialitetit*", në përmbushje të detyrimit ligjor që buron nga neni 28 i 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 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 hetimit administrativ hartoi procesverbalin përkatës, një kopje e të cilit i është vënë në dispozicion Kontrolluesit.

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 në datë 19.11.2024, paraqiti pretendimet mbi konstatimet e procesverbalit duke bashkëlidhur dhe provat si:

1. GDPR DPIA assessment;
2. Sinteza Co Cybersecurity Protection Plan;
3. Tabela e informimit për sistemin e video-survejimit CCTV;
4. Nas backup + HDD (1TB)
5. Manual lidhur me trajnimet e personelit;

Adresa: Rruga *"Abdi Toptani"*, Nd.5, Tiranë Telefon: +355 42237200 www.idp.al, info@idp.al

- General Data Protection Regulation (GDPR) Kursi i Ndërgjegjësimit;
- GDPR Workbook;
- Pyetësori i Ndërgjegjësimit për GDPR Niveli 1, si dhe lista e stafit të trajnuar;
- Formularë Vlerësimi;
- Deklarata e trajnimit;

- Lidhur me "*Politikat e Privatësisë*" në web dhe me "*Deklaratën e Konfidencialitetit*", Kontrolluesi deklaroj se janë në proces implementimi.

- Lidhur me pikën 7 të konstatimeve, Kontrolluesi deklaron se "...*janë marrë masa të menjëhershme dhe janë implementuar, në përputhje me rregullat përkatëse. Sa i përket arkivës, ekipi teknik është në proces implementimi të pajisjes NAS dhe të të gjithë masave teknike për t'u përputhur me kërkesat (parashikohet brenda 20 ditëve)".*

- Lidhur me tabelën "*Për sistemin e video-survejimit CCTV*", Zyra e Komisionerit konstaton se tabela e vendosur nga Kontrolluesi nuk është formati i miratuar sipas Udhëzimit nr. 3 të Komisionerit.

  Zyra e Komisionerit vlerëson se, subjektet e të dhënave duhet të informohen qartësisht që një sistem video-survejimi është në veprim, duke vendosur në ambientet e survejuara modelin standard të tabelës informuese për mbikëqyrjen me sistemin e survejimit, të miratuar nga Komisioneri.

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

a) kontrolluesit, që përdorin të dhëna personale në kundërshtim me kreun II "Përpunimi i të dhënave personale", dënohen me 10 000 deri në 500 000 lekë;
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;
ç) kontrolluesit ose përpunuesit, që nuk zbatojnë detyrimet e përcaktuara në nenin 20 tëkëtij 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

Adresa: Rruga *"Abdi Toptani"*, Nd.5, Tiranë Telefon: +355 42237200 www.idp.al, info@idp.al

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 5, 18, 20, 21, 27, 28, 29, 30, 39 pika 1, *"a"; "b", "ç"; "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 60 000 (gjashtëdhjetë mijë) lekë, për shkelje të detyrimeve të përcaktuara në Kreun II të Ligjit;

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

3- Dënimin e Kontrolluesit me gjobë në vlerën 60 000 (gjashtëdhjetë mijë) lekë, për shkelje të detyrimit të përcaktuar në nenin 20 të Ligjit;

4- Dënimin e Kontrolluesit me gjobë në vlerën 40 000 (dyzet mijë) lekë, për shkelje të detyrimit të përcaktuar në nenin 21 të Ligjit;

5- Dënimin e Kontrolluesit me gjobë në vlerën 60 000 (gjashtëdhjetë mijë) lekë, për shkelje të detyrimit të përcaktuar në nenet 27 dhe 28 të Ligjit;

6- Kontrolluesi, të marrë masa për të përcaktuar afatet kohore për ruajtjen e të dhënave, për të gjithë proceset e përpunimit, në përputhje me germën *"d"*, të pikës 1, të nenit 5 të Ligjit;

7- Kontrolluesi, në zbatim të nenit 18 të Ligjit, si dhe Udhëzimit nr. 3 të Komisionerit, të marrë masa për vendosjen e tabelës për sistemin e video-survejimit CCTV, sipas modelit të miratuar;

8- 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;

9- 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;

10- 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;

11- 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

Adresa: Rruga *"Abdi Toptani"*, Nd.5, Tiranë Telefon: +355 42237200 www.idp.al, info@idp.al

administrimit të Sistemit të Menaxhimit të Sigurisë së Informacionit (SMSI) për mbrojtjen e të dhënave personale;

12- 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;

13- Kontrolluesi, në zbatim të nenit 28 të Ligjit, të hartojë dhe aplikojë për punëmarrësit "*Deklaratën e Konfidencialitetit*";

14- Në zbatim të pikës 1 të nenit 32 të Ligjit, të përmbushen detyrimet, sipas këtij akti brenda afateve, si vijon:

i. Vazhdimisht, detyrimet e përcaktuara në pikën 10 më sipër;
ii. brenda 15 (pesëmbëdhjetë) ditëve, detyrimet e përcaktuara në pikat 6, 7, 8 dhe 13 më sipër;
iii. brenda 30 (tridhjetë) ditëve, detyrimet e përcaktuara në pikën 9 më sipër;
iv. brenda 45 (dyzetë e pesë) ditëve, detyrimet e përcaktuara në pikën 11 më sipër.

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

15- Kontrolluesi të njoftojë Zyrën e Komisionerit për masat e marra;

16- Gjoba 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 Përmbarimit;

17- 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

Adresa: Rruga *"Abdi Toptani"*, Nd.5, Tiranë Telefon: +355 42237200 www.idp.al, info@idp.al