Nr.161/1 prot. Tiranë më 17.01.2023

REKOMANDIM

Nr. 01, datë 17.01.2023

PËR KONTROLLUESIN "*EASYPAY SH.P.K*"

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*"), 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 *"EasyPay SH.P.K"* (në vijim, *"Kontrolluesi"*),

KONSTATOVA SE:

Në zbatim të Urdhrit nr. 204, datë 24.11.2022, të Komisionerit për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale, 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) dhe verifikim rekomandimi.

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

1. Kontrolluesi ushtron veprimtari financiare jobankare, sipas përcaktimeve në kuadrin ligjor dhe rregullator për institucionet financiare jobankare, të tilla si kredidhënia, mikrokredia, faktoringu, qiraja financiare, shërbimi i pagesave dhe transferimit të parave, emetimi i parasë elektronike, këmbimi valutor, etj.

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

Në kuadër të veprimtarisë që kryen, Kontrolluesi përpunon të dhëna personale për kategoritë, *"punonjës", "vizitorë", "kandidatë për punë", "klienta",* etj. Përpunimi i të dhënave kryhet në mënyrë manuale dhe elektronike.

Gjatë ushtrimit të aktivitetit, Kontrolluesi përdor sistemin elektronik/platformën EasyVoucher për agjentë, klientët dhe nëpunësit. Easy Voucher është sistemi për përdorim nga Agjentët në të cilën kryhen shërbimet për pagesat online për subjektet e të dhënave si, të energjisë elektrike, gjobat e automjeteve, furnizimit me ujë, rimbushje telefonike, etj. Gjithashtu, Easy Voucher clients është sistemi elektronik/platforma që kryhen të njëjtat shërbime si EasyVoucher për agjentë por që përdoret nga vetë strukturat e nëpunësve të klientëve përfitues. Riapay Online ofrohet nga Ria Money Transfer, është vetëm për transfertat ndërkombëtare të parave.

Sistemi/platforma Easy Voucher është i ngritur mbi:

- Sistemin e Operimit Windows Server 2012 /Windows Server 2019;
- Serverat funksionojnë sipas modelit redundant server;
- Sistemi/platforma Easy Voucher hostohet në site primar dhe në një site sekondar;
- Hyper-V funksionon me replica failover. Ekzistojnë nyje të njëjta të cilat mbajnë VM përkatëse. Secila VM te nyjet jo burim, replikohet në mënyre automatike nga Hyper V service;
- Network i është i përberë nga dy firewall të ndryshëm që janë të ndarë për funksionalitete të ndryshme . Dy firewallet janë Cisco ASA 5510 dhe Fortigate 200E, ku ASA është në funksion për serverat dhe për lidhjet VPN S2S që ka me partnerët. Ndërsa Fortigate është në funksion për end users (stafi, wifi, printers, DVR, alarm systems, access control).

Sistemi/platforma EasyVoucher ndërvepron gjithashtu me sistemet elektronike të palëve të treta të tilla si Drejtorinë e Përgjithshme të Taksave dhe Tarifave Vendore, OSHEE, etj. Çdo klient ka një portofol (llogari) pranë EasyPay, në të cilën kalojnë pagesat respektive nga palët e treta.

2. Konstatohet se të dhënat e ish punëmarrësve ruhen pa afat edhe në arkivin fizik të Kontrolluesit. Përmbajtja e dosjeve personale të ish punëmarrësve, konsiston në dokumente origjinale, të noterizuara dhe/ose të fotokopjuara, të tilla si: jetëshkrime, kopje të kartës së identitetit, raport mjeko ligjor, certifikata familjare dhe personale, vërtetim të gjendjes gjyqësore, etj.

   Kontrolluesi nuk ka parashikuar asnjë afat konkret për mbajtjen e të dhënave personale, në kundërshtim me parimet e mbrojtjes së të dhënave personale dhe kriteret ligjore për përpunimin e të dhënave, të parashikuara në nenet 5 dhe 6 të Ligjit dhe Udhëzimin nr. 11 datë 08.09.2011 *"Për përpunimin e të dhënave të punonjësve në sektorin privat",* i ndryshuar (në vijim, *"Udhëzimi nr. 11"*).

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

Gjithashtu, Kontrolluesi gjatë procesit të përpunimit të të dhënave për kategorinë e subjekteve kandidatë për punë, nuk ka respektuar parimin e mbrojtjes së të dhënave personale lidhur me kohën e ruajtjes së të dhënave personale. Të dhënat për këtë kategori subjektesh përpunohen nëpërmjet sistemit elektronik që nga koha e fillimit të aktivitetit, pavarësisht se këto subjekte janë klasifikuar si të papërshtatshëm për tu punësuar më tej.

Zyra e Komisionerit vlerëson se, Kontrolluesi ka detyrim të përpunojë të dhënat personale për aq kohë sa ekziston qëllimi për të cilin janë grumbulluar dhe përpunuar (neni 5/1/d) dhe në momentin që qëllimi ka përfunduar, të realizojë shkatërrimin e tyre, në të kundërt përpunimi i mëtejshëm i të dhënave konsiderohet i paligjshëm.

3. Kontrolluesi disponon faqen online https://www.easypay.al, në të cilën konstatohet të jetë i publikuar dokumenti *"Politikat dhe detyrimet ligjore"*, në të cilën, në pikën 12 të saj, përmban një informacion të përgjithshëm mbi *"Përdorimin e të dhënave personale".* Nga shqyrtimi i përmbajtjes së këtij dokumenti, rezulton se është e njëjta përmbajtje sikurse dokumenti *"Kushtet dhe afatet e ofrimit të shërbimeve EasyPay".* Përmbajtja e pikës 12 ka për qëllim udhëzimin e klientit për përdorimin e fjalëkalimit të llogarisë elektronike në EasyPay.

Kontrolluesi nuk ka publikuar *"Politikat e Privatësisë"* në faqen https://www.easypay.al, me qëllim informimin e subjekteve të të dhënave personale, mbi qëllimin dhe mënyrën e përpunimit të të dhënave, personin që do t'i përpunojë, të drejtat ligjore që gëzojnë, afatin e mbajtjes së të dhënave, nëse dhënia e të dhënave personale është e detyrueshme apo vullnetare, të drejtën për të kundërshtuar përpunimin e mëtejshëm të tyre, 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. Mos përmbushja 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.

4. Kontrolluesi ka miratuar një grup politikash lidhur me, sigurinë e informacionit. Konkretisht ka hartuar:

- Siguria e informacionit EasyPay;
- Procedura fjalëkalimeve;
- Procedurë për disaster dhe recovery sight (e pa miratuar);
- Business continue plan / disaster recovery plan;
- Information security-ISM;
- Politikë dhe procedurë për backup;

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

- Politikë e menaxhimit të aksesit dhe të përdoruesve;
- Procedurë menaxhimi të ndryshimeve në IT;
- Service Management system policy;
- Design and transition of new change services;
- Service design package for service name;
- Service level management process;
- Service level agreement (SLA) template;
- Operational level agreement (OLA) template;
- Budgeting and accounting for services;
- Business relationship management;
- Supplier management;
- Incident and service request management;
- Change management SMS-11;
- Change management policy;
- Configuration management.

Konstatohet se masat e ndërmarra nga Kontrolluesi janë të pamjaftueshme në raport më veprimtarinë e gjerë që kryen. Grupi i kontrollit konstaton mosplotësim të detyrimeve në lidhje me ngritjen, administrimin dhe mirëmbajtjen e sistemit të menaxhimit të sigurisë së informacionit (SMSI) lidhur me mbrojtjen e të dhënave personale, sipas parashikimeve të Udhëzimit nr. 47 të Komisionerit, 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"*), për shkak të cilësisë si subjekt përpunues i madh, si dhe për shkak të natyrës së veçantë të veprimtarisë që Kontrolluesi ushtron.

Konkretisht, konstatohet se mungojnë elementë të tjerë të sigurisë së të dhënave si, *"Dokumentimi i proceseve të politikave të miratuara nga Kontrolluesi", "Kontrollin e sigurisë së sistemit të përpunimit të të dhënave personale nga një audites i pavarur", "Analiza e sigurisë së sistemit të arkivimit", "Analizë e ndikimit në të dhëna personale", "Raport vlerësimi mbi sigurinë në sistemin e arkivimit",* në kundërshtim me parashikimet e nenit 27 të Ligjit dhe Udhëzimit nr. 47.

Zyra e Komisionerit vlerëson se, zbatueshmëria dhe dokumentimi i procedurave dhe politikave në lidhje më sigurinë e informacionit, është një ndër masat kryesore që duhet të ndërmarrë Kontrolluesi, në lidhje me sigurinë dhe funksionimin e sistemeve të teknologjisë së informacionit. Gjithashtu, (SMSI) lidhur me mbrojtjen e të dhënave personale, duhet të jetë në përputhje me parashikimet e Udhëzimit nr. 47 të Komisionerit.

Kontrolluesi ka ndërmarrë 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, megjithatë, nga verifikimi i përmbajtjes së manualit trajnues,

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

rezulton se përmbajtja e tij nuk është e mjaftueshme, dhe ka nevojë të përfshijë të gjitha proceset përpunuese të Kontrolluesit.

Zyra e Komisionerit vlerëson se trajnimet në lidhje me mbrojtjen e të dhënave personale duhet të jenë të vazhdueshme dhe të përshtatura sipas nevojave dhe proceseve të punës të Kontrolluesit, me qëllim ndërgjegjësimin e operatorëve të cilët për shkak të proceseve të punës, janë të ngarkuar për përpunimin e të dhënave personale.

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 dërguar Kontrolluesit me rrugë 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. Përfaqësuesit e Kontrolluesit janë paraqitur në seancën dëgjimore datë 05.01.2023, të organizuar nga Zyra e Komisionerit dhe kanë deklaruar angazhimin për rikuperimin e shkeljeve të konstatuara gjatë hetimit administrativ.

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, 27, 29, 30, 31 (pika 1, germa *"a/l"*), si dhe 32 të Ligjit,

REKOMANDOJ:

1. Kontrolluesi, në përputhje me parimet dhe kriteret ligjore të përpunimit të sanksionuara në nenet 5 dhe 6 të Ligjit, të marrë masa për shkatërrimin e të dhënave të ruajtura/mbledhura në tejkalim të qëllimit të përpunimit për të cilat janë mbledhur;

2. Kontrolluesi, të ketë në vëmendje përpunimin e të dhënave personale në përputhje me parimet dhe kriteret ligjore të sanksionuara në nenet 5 dhe 6 të Ligjit;

3. 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;

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

4. Kontrolluesi, të marrë masa konkrete teknike dhe organizative për mbrojtjen e të dhënave personale, në përputhje me parashikimet e nenit 27 të Ligjit dhe Udhëzimin 47;

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

   (i) brenda 5 (pesë) ditëve, detyrimet e treguara në pikën 1 më sipër;
   (ii) vazhdimisht, detyrimet e treguara në pikën 2 dhe 3 më sipër;
   (iii) brenda 45 (dyzetë e pesë) ditëve, detyrimet e përcaktuara në pikën 4 dhe 5 më sipër.

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

6. Kontrolluesi të njoftojë Komisionerin për masat e marra;

7. Në rast mos përmbushje 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 17.01.2023.

KOMISIONERI

Besnik Dervishi

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