Projekt – twinning i BE-së "Mbështetje në zbatimin e kornizës së modernizuar ligjore për mbrojtjen e të dhënave personale"

10 HAPA TË SHPEJTË PËR HARMONIZIM

me Ligjin për mbrojtjen e të dhënave personale

1. IDENTIFIKONI LËVIZJEN E TË DHËNAVE PERSONALE NË ORGANIZATËN
2. IDENTIFIKONI BAZËN JURIDIKE
3. MBANI EVIDENCË PËR AKTIVITETET PËR PËRPUNIMIN E TË DHËNAVE PERSONALE, NËSE ËSHTË E ZBATUESHME
4. CAKTONI OFICER PËR MBROJTJEN E TË DHËNAVE PERSONALE, NËSE ËSHTË E ZBATUESHME
5. POLITIKA / NJOFTIMI / DEKLARATA PËR PRIVATËSI
6. SHQYRTONI TË DREJTAT PËR MBROJTJEN E TË DHËNAVE PERSONALE
7. BËNI VLERËSIMIN E NDIKIMIT MBI MBROJTJEN E TË DHËNAVE PERSONALE, NËSE ËSHTË E ZBATUESHME
8. BËNI PLAN ME SKENAR ME CENIM TË SIGURISË SË TË DHËNAVE PERSONALE
9. ZBATONI MASAT TEKNIKE DHE ORGANIZATIVE ADEKUATE
10. DEKLARATAT PËR KONFIDENCIALITET

Ky publikim u mundësua me përkrahje financiare të Bashkimit Evropian. Përmbajtja është përgjegjësi e autorit dhe jo domosdoshmërisht paraqet pikëpamjet të Bashkimit Evropian.

1. IDENTIFIKONI LËVIZJEN E TË DHËNAVE PERSONALE NË ORGANIZATËN

Është e rëndësishme që kontrolluesit të bëjnë regjistrimin e të gjitha të dhënave personale që i posedojnë. Kontrolluesit duhet ta skanojnë situatën në organizatën e tyre dhe të dokumentojnë pse u duhen të dhënat personale që i përpunojnë, t'i përcaktojnë qëllimet e përpunimit dhe të garantojnë sigurinë e përpunimit.

Shembull:

Barnatorja kryen shitjen në lokacionin fizik në qendër të qytetit dhe përmes ueb-shitores. Ajo ka edhe ueb-faqen e saj. Para se të bëjnë porosinë-online, blerësve u ofrohet anëtarësia në programin për lojalitet i cili mundëson lirim gjatë blerjes, por edhe njoftime të rregullta për produktet e barnatores. Për aktivitetet e tyre afariste, barnatorja shfrytëzon sistem kontabiliteti, dhe ka sistem për video-mbikëqyrje për sigurimin e pronës, të të punësuarve dhe blerësve.
Si rrjedhojë, të paktën, barnatorja mbledh informata të kontaktit për blerësit që shfrytëzohen për dërgimin e njoftimeve për produktet.
Kur konsumatorët bëjnë porosi-online, ata duhet t'i lënë të dhënat si vijojnë: emrin, mbiemrin dhe adresën për dërgimin e produkteve.
Përveç kësaj, në ueb-faqen e barnatores janë instaluara të a.q. biskota (cookies) të palëve të treta, që mbledhin informata personale për qëllime marketingu.
Në kuadër të programit të kontabilitetit, barnatorja përpunon të dhëna personale të të punësuarve për qëllimet e pagimit të rregullt të rrogave, ndërsa përmes sistemit për video-mbikëqyrje mblidhen të dhëna personale për vizitorët dhe të punësuarit.

Rekomandohet që kontrolluesit të bëjnë regjistrimin e të gjitha të dhënave personale që i ruajnë dhe i dokumentojnë çështjet si vijojnë:

a. Si janë marrë të dhënat personale?
b. Pse ruhen të dhënat e tilla?
c. Nëse të dhënat personale janë ende të nevojshme?
ç. Nëse të dhënat personale janë të sigurta?
d. Me kë ndahen të dhënat personale?

Pas skanimit të situatës, kontrolluesi duhet të bëjë hartë se si lëvizin të dhënat personale në organizatën e tij që të sigurojë kontroll më të madh të aktiviteteve afariste.
Mbani mend, ky aktivitet ndihmon edhe në mbajtjen e reputacionit të biznesit.

2. IDENTIFIKONI BAZËN JURIDIKE

Për çdo përpunim të të dhënave personale duhet të ekzistojë bazë juridike për përpunimin e dhënë në nenin 10, paragrafi (1) të Ligjit për mbrojtjen e të dhënave personale.
Kontrolluesi duhet të identifikojë bazën juridike për përpunimin, të dokumentojë dhe t'i informojë personat fizikë për të në kuadër të politikës / njoftimit / deklaratës së tij për privatësi.

Ky projekt financohet
nga Bashkimi Evropian

Duhet të kihet parasysh se nëse kontrolluesi bazohet në pajtimin nga personat fizikë si bazë juridike për përpunimin e të dhënave personale, atëherë ai duhet të garantojë se janë përmbushur të gjitha kushtet e përcaktuara me ligj. Gjithashtu, nëse përpunimi përfshin kategori të veçanta të të dhënave personale (p.sh. të dhënat biometrike, të dhënat gjenetike, të dhënat të cilat kanë të bëjnë me shëndetin), kontrolluesi duhet t'i referohet bazës juridike për përpunimin e dhënë në nenin 10, paragrafi (1) të Ligjit për mbrojtjen e të dhënave personale, dhe një nga përjashtimet për përpunimin e të dhënave të tilla të dhëna në nenin 13 të Ligjit për mbrojtjen e të dhënave personale.

Shembull:
Kompania vendos sistem elektronik me skanimin e gjurmëve të gishtit për hyrje në hapësirat e saj. Ky sistem paraqet përpunimin e të dhënave biometrike për identifikimin e orëve të punës të të punësuarve. Kompania duhet t'i përmbush kushtet përkatëse për përpunimin e kategorisë së veçantë të të dhënave personale (baza juridike e dhënë në nenin 10, një nga përjashtimet për përpunimin e të dhënave të tilla personale të dhëna në nenin 13, dhe përmbushjen e kushteve të përcaktuara në nenin 84 të Ligjit për mbrojtjen e të dhënave personale).

3. MBANI EVIDENCË PËR AKTIVITETET PËR PËRPUNIMIN E TË DHËNAVE PERSONALE, NËSE ËSHTË E ZBATUESHME

Në disa raste, kontrolluesi / përpunuesi duhet të mbajë evidencë për aktivitetet e tij për përpunimin e të dhënave personale e cila, mes tjerash, përfshin informata për qëllimet e përpunimit, kategoritë e subjekteve të të dhënave personale, kategoritë e të dhënave personale, kategoritë e pranuesve të të dhënave personale, transferimin e të dhënave personale, afatin për fshirjen e të dhënave personale, masat teknike dhe organizative.
Ky lloj i evidencës është mënyrë e shkëlqyer për vendosjen e kontrollit mbi përpunimin dhe lëvizjen e të dhënave personale te kontrolluesi. Ruajtja e këtyre informatave në një vend e lehtëson harmonizimin me Ligjin për mbrojtjen e të dhënave personale.

Shembull: sistemi për video-mbikëqyrje

Kontrollues: Kompania SHPKPV

Kategoria e subjekteve dhe kategoria e të dhënave personale: video incizime nga vizitorët e Kompanisë SHPKPV, të cilat përmbajnë karakteristika të fizionomisë së ndonjë personi.

Qëllimi: mbrojtja e pronësisë, mbrojtja e jetëve dhe shëndetit të të punësuarve për shkak të natyrës së punës që kryhet.

Pranues: Kompania HL SHPKPV. **Afati për fshirjen e të dhënave:** 30 ditë

Masat teknike dhe organizative: akti i veçantë për mënyrën e kryerjes së video-mbikëqyrjes (p.sh. autorizimi për qasjen te incizimet, sistemi i automatizuar i regjistrimeve (kyçjeve), transparencës), sistemi i mbrojtur me fjalëkalim, trajnimi për të punësuarit, etj.

Transferimi i të dhënave personale: /

Ky projekt financohet
nga Bashkimi Evropian

4. CAKTONI OFICER PËR MBROJTJEN E TË DHËNAVE PERSONALE, NËSE ËSHTË E ZBATUESHME

Disa kontrollues janë të obliguar të caktojnë oficer për mbrojtjen e të dhënave personale.

Obligimi i tillë ekziston në rastet si vijojnë:

- kur përpunimin e të dhënave personale e kryejnë organet e administratës shtetërore (përveç gjykatave, kur veprojnë në kuadër të kompetencave të tyre);
- kur veprimtaria bazë e kontrolluesit përbëhet nga operacionet për përpunimin e vëllimshëm të cilat imponojnë ndjekjen e rregullt dhe sistematike të personave fizikë (p.sh. kompania për sigurim e cila ka sistem për video-mbikëqyrje në disa qendra tregtare); dhe
- kur veprimtaria bazë e kontrolluesit përfshin përpunimin e vëllimshëm të kategorive të veçanta të të dhënave personale (si p.sh. të dhënat biometrike, të dhënat gjenetike, të dhënat të cilat kanë të bëjnë me shëndetin) ose të dhënat personale lidhur me aktgjykimet e dënueshme dhe veprat penale (si p.sh. aktivitetet për përpunimin e të dhënave personale në spital konsiderohen përpunim i vëllimshëm kundrejt përpunimit që e kryen mjeku, që nuk konsiderohet për përpunimin e vëllimshëm të të dhënave personale).

Oficeri për mbrojtjen e të dhënave personale duhet të përcaktohet në bazë të kualifikimeve dhe njohurive të tij / të saj profesionale në fushën e mbrojtjes së të dhënave personale. Gjithashtu, oficeri duhet të jetë i njoftuar me praktikat më të mira dhe të jetë i aftë t'i kryejë detyrat e punës dhe detyrimet e përcaktuara me ligj.

Ligji për mbrojtjen e të dhënave personale përcakton kushte të veçanta për personin që përcaktohet si oficer për mbrojtjen e të dhënave personale:

- t'i përmbush kushtet për punësim të përcaktuar me Ligjin për mbrojtjen e të dhënave personale dhe me ligj tjetër;
- në mënyrë aktive ta përdor gjuhën maqedonase;
- në momentin e caktimit, me aktgjykim të plotfuqishëm gjyqësor të mos i është shqiptuar dënimi ose sanksioni kundërvajtës për ndalimin për kryerjen e profesionit, veprimtarisë ose detyrës;
- të ketë më së paku 240 kredi sipas Sistemit Evropian të Transferit të Kredive (SETK) ose të ketë mbaruar shkallën VII/1 të arsimit të lartë;
- të ketë fituar njohuri dhe shkathtësi në lidhje me praktikat dhe rregullat në fushën e mbrojtjes së të dhënave personale.

Përveç kualifikimeve profesionale, cilat janë kushtet tjera të përcaktuara për oficerin për mbrojtjen e të dhënave personale?

Grup kompanish mund të caktojnë një oficer për mbrojtjen e të dhënave personale, me kusht ai / ajo të jetë e barabartë dhe lehtë në dispozicion për të gjithë personat juridikë nga grupi dhe për subjektet e të dhënave personale, derisa në rast të organeve të administratës shtetërore, një oficer mund të caktohet për disa organe në përbërjen e organit kompetent.

Oficeri për mbrojtjen e të dhënave personale mund të jetë personi i punësuar ose t'i kryejë detyrat e punës në bazë të marrëveshjes.

Ky projekt financohet
nga Bashkimi Evropian

Duhet të vërehet se, edhe pse oficerët për mbrojtjen e të dhënave personale mund të kryejnë edhe detyra dhe detyrime tjera, angazhimi i tillë nuk mund të rezultojë me konfliktin e interesave, sepse mungesa e konfliktit të tillë konsiderohet kryerje e pavarur e detyrave dhe detyrimeve.

Për këto arsye, oficeri nuk guxon të jetë person i punësuar i cili merr pjesë në përcaktimin e qëllimeve dhe metodave të përpunimit të të dhënave personale.

Përveç kësaj, nuk këshillohet që personat në pozicionet e caktuara në kuadër të kompanisë që mund të kenë konflikt të interesave të caktohen si oficerë për mbrojtjen e të dhënave personale, si për shembull, personat që kryejnë pozicione të larta menaxheriale (drejtor ekzekutiv, drejtor operativ kryesor), udhëheqësit e seksioneve për marketing, udhëheqësit e seksioneve për menaxhim me resurset njerëzore, administratori i sistemit të informacionit etj., por edhe personat që kanë pozicione më të ulëta në kuadër të kompanisë, nëse pozicioni i tillë nënkupton përcaktimin e qëllimeve dhe metodave për përpunimin e të dhënave personale.

Detyrat e oficerit për mbrojtjen e të dhënave personale përfshijnë dhënien e këshillave kontrolluesit për të gjitha çështjet në fushën e mbrojtjes së të dhënave personale.

Kontrolluesi dhe përpunuesi duhet të sigurohen se oficeri për mbrojtjen e të dhënave personale është adekuatë dhe në kohë i përfshirë në të gjitha çështjet në fushën e mbrojtjes së të dhënave personale.

Sipas ligjit, detyrat dhe detyrimet e oficerit për mbrojtjen e të dhënave personale përfshijnë edhe ndjekjen e harmonizimit dhe trajnimin e të punësuarve.

Për këto arsye, oficeri për mbrojtjen e të dhënave personale është me vlerë të madhe për çdo organizatë, dhe prandaj Agjencia për Mbrojtjen e të Dhënave Personale rekomandon oficerë të tillë të caktohen edhe kur personat juridikë nuk kanë obligim të tillë.

Shënim i rëndësishëm! Kontrolluesi ose përpunuesi është i detyruar, në ueb-faqen e tyre, t'i publikojë detajet e kontaktit për oficerin për mbrojtjen e të dhënave personale dhe t'i dorëzojë në Agjencinë për Mbrojtjen e të Dhënave Personale.

Shembull:
Organet e administratës shtetërore, siç janë ministritë, institutet, institucionet, etj., duhet të caktojnë oficer për mbrojtjen e të dhënave personale.

5. POLITIKA / NJOFTIMI / DEKLARATA PËR PRIVATËSI

Politika / njoftimi / deklarata për privatësi e personave fizikë u siguron informata në mënyrë të qartë, koncize, transparente, të kuptueshme dhe lehtë të disponueshme, dhe me shfrytëzimin e gjuhës së rëndomtë, që përshkruajnë si kontrolluesi i përpunon të dhënat personale.

Kontrolluesit duhet t'i informojnë personat fizikë për qëllimet e përpunimit, bazën juridike për përpunim, afatin për ruajtje, nëse të dhënat personale ndahen me personat tjerë juridikë dhe fizikë, interesin legjitim të kontrolluesit ose të ndonjë pale të tretë, qëllimin e kontrolluesit për transferimin e të dhënave personale te vendet e treta ose organizatat ndërkombëtare, detajet e kontaktit të oficerit për mbrojtjen e të dhënave personale, etj.

Ky projekt financohet
nga Bashkimi Evropian

Shembull:

Marija është parukiere. Ajo nuk ka ueb-faqe, por ka vendosur njoftim në sallonin në të cilin thuhet se klientët mund të kërkojnë kopjen e deklaratës së saj për privatësi.

Kompania XX SHPKPV punon dizajn grafik. Ajo ka ueb-faqen e saj në të cilën, në vend të dukshëm, është publikuar deklarata për privatësi.

Të dy kontrolluesit kanë deklaratë për privatësi e cila është përbërë nga të gjitha elementet e përcaktuara me Ligjin për mbrojtjen e të dhënave personale (neni 16, 17, dhe 18).

6. SHQYRTONI TË DREJTAT PËR MBROJTJEN E TË DHËNAVE PERSONALE

Kontrolluesi duhet të jetë i vetëdijshëm se personat fizikë gëzojnë të drejta të caktuara, dhe atë: së pari duhet të jenë të informuar; e drejta e qasjes, korrigjimi dhe fshirja e të dhënave personale; e drejta e kufizimit të përpunimit; transferimi i të dhënave; e drejta e kundërshtimit, dhe e drejta të mos jetë lëndë e vendimit të bazuar vetëm në përpunimin e automatizuar, duke përfshirë edhe profilimin.

Është e rëndësishme që kontrolluesi duhet të jetë i njoftuar me këto të drejta dhe në mënyrë adekuate t'i planifikojë politikat e tyre.

Shembull:

Ish-i punësuari në një organizatë nga punëdhënësi kërkon t'i fshijë të gjitha të dhënat e tij personale.

Organizata mund ta refuzojë kërkesën për fshirjen e të dhënave personale të ish-të të punësuarve, nëse ende ekziston detyrimi ligjor për përpunimin e të dhënave të tilla..

7. BËNI VLERËSIMIN E NDIKIMIT MBI MBROJTJEN E TË DHËNAVE PERSONALE, NËSE ËSHTË E ZBATUESHME

Vlerësimi i ndikimit mbi mbrojtjen e të dhënave personale i ndihmon kontrolluesit t'i identifikojë dhe t'i minimizojë rreziqet për mbrojtjen e të dhënave personale, dhe ajo konsiderohet mjet kyç për llogaridhënie.

Shembull:

Në disa raste, aplikacionet e caktuara nga "Interneti i gjërave" mund të kenë ndikim të madh mbi të drejtat dhe liritë e personit fizik për mbrojtjen e të dhënave personale dhe prandaj aplikacionet e tilla mund të imponojnë vlerësimin e ndikimit mbi mbrojtjen e të dhënave personale.

Ky projekt financohet nga Bashkimi Evropian

8. BËNI PLAN ME SKENAR ME CENIM TË SIGURISË SË TË DHËNAVE PERSONALE

Në rast të cenimit të sigurisë së të dhënave personale, kontrolluesi duhet menjëherë, por jo më vonë se 72 orë pasi ka kuptuar për cenimin ta njoftojë Agjencinë për Mbrojtjen e të Dhënave Personale në **Incident@privacy.mk** ose **https://eprijavi.privacy.mk/.**

Kjo është një nga sfidat më të mëdha për kontrolluesit, ndërsa njoftimi që dorëzohet në Agjencinë për Mbrojtjen e të Dhënave Personale duhet të jetë në detaje.

Nëse nuk ka mundësi për njoftimin e Agjencisë për Mbrojtjen e të Dhënave Personale në afat prej 72 orësh, kontrolluesi mund ta dorëzojë njoftimin gradualisht, pa prolongim të panevojshëm më tej. Ky obligim nuk zbatohet në rastet ku nuk ka probabilitet se cenimi i sigurisë së të dhënave personale do të rezultojë me rrezik të madh për të drejtat dhe liritë e personave fizikë.

Shembull:

Një komunë shpall thirrje për përkrahjen e shoqatave që u sigurojnë ndihmë personave të vjetër dhe personave të pafuqishëm. Në thirrje janë paraqitur më shumë shoqata, ndërsa disa prej tyre kanë arritur të marrin përkrahje financiare nga komunat për aktivitetet e tyre.

Kur komuna i ka njoftuar shoqatat që kanë marrë përkrahje (përmes e-meilit), ajo rastësisht i ka vënë kontaktet e të gjitha shoqatave në pjesën për karbon kopje (cc:) në vend se në pjesën për kopje të padukshme (bcc:) me çka do të ishte penguar zbulimi i të dhënave personale të personave të paautorizuar.

Edhe pse kjo paraqet shkelje, nuk ekziston rrezik i madh për personat fizikë (disa e-meil adresa kanë përmbajtur emrin e personit për kontakt nga shoqata relevante, por përmbajtja e mesazhit nuk ka qenë konfidenciale / ndjeshme), prandaj ky incident nuk duhet të paraqitet në Agjencinë për Mbrojtjen e të Dhënave Personale.

Komuna e ka dokumentuar këtë prishje të sigurisë së të dhënave personale, duke përfshirë edhe faktet dhe efektet e ngjarjes, si dhe veprimet korrigjuese që i ka ndërmarrë.

9. ZBATONI MASAT TEKNIKE DHE ORGANIZATIVE ADEKUATE

Që të sigurohet niveli i sigurisë që është adekuat me rrezikun dhe të pengohet skenari për cenimin e sigurisë së të dhënave personale, kontrolluesi duhet të zbatojë masa adekuate për siguri.

Agjencia për Mbrojtjen e të Dhënave Personale rekomandon masa siç janë: ruajtja e sigurt e dokumenteve në kopje në letër që përmbajnë të dhëna personale, për shembull, në sirtarë me bravë me kyçje; dhënia e qasjes në të dhënat personale që ruhen në formën elektronike vetëm për personat e autorizuar; këshilla për të punësuarit që të shfrytëzojnë fjalëkalime komplekse, bërja e rregullt e kopjeve të sigurisë së evidencave elektronike; pseudonimi ose kriptimi i të dhënave personale, posaçërisht në rast të kategorive të posaçme të të dhënave personale.

Përveç kësaj, është me rëndësi që çështje të caktuara të jenë të rregulluara përmes akteve nënligjore dhe procedurave interne të kontrolluesit, dhe në fund, por jo më pak e rëndësishme, të punohet në rritjen e vetëdijes

Ky projekt financohet
nga Bashkimi Evropian

në kuadër të organizatës, sepse përqindja e madhe nga prishjet e sigurisë së të dhënave personale ndodhin për shkak të gabimeve të njeriut

Shembull:

Në lidhje me sigurinë e të dhënave personale, kontrolluesi duhet të marrë përgjegjësi për përpunimin dhe zbatimin e politikave dhe procedurave për siguri, si dhe trajnimin e të punësuarve. Gjithashtu, kontrolluesi duhet të kontrollojë nëse janë ndërmarrë masa të sigurisë dhe duhet të bëhet hetimi në rast të cenimit të sigurisë.

10. DEKLARATAT PËR KONFIDENCIALITET

Kontrolluesi duhet të kërkojë nga të punësuarit dhe furnizuesit të nënshkruajnë deklaratë për konfidencialitet me të cilën obligohen në konfidencialitetin e të dhënave personale gjatë kryerjes së punës së tyre. Në atë mënyrë, kontrolluesi e garanton sigurinë e të dhënave personale në kuadër të punës së tij.

Shembull:

Në cilësinë e funksionarit / të të punësuarit në organin / kompaninë _____, unë i poshtë nënshkruari _____ deklaroj se do ta respektoj konfidencialitetin e të gjitha të dhënave personale për të cilat kam të drejtë dhe autorizim për qasje dhe të cilat ruhen në përmbledhjen e të dhënave personale në organin / kompaninë ku e kryej pozicionin e punës, dhe se do t'i përpunoj të dhënat personale vetëm për qëllimet konkrete, qëllimet e përcaktuara ligjore, në pajtim me Ligjin për mbrojtjen e të dhënave personale, veçanërisht në pajtim me parimin e konfidencialitetit nga neni 9 të ligjit.

Gjithashtu, obligohem se nuk do të dorëzoj ose në çfarëdo mënyre tjetër t'i vë në dispozicion palëve të treta të dhënat personale për të cilat kam të drejtë dhe autorizim për qasje (zbulimi i paautorizuar), dhe se obligohem se do ta ruaj konfidencialitetin e të dhënave personale edhe pas shfuqizimit të autorizimit për qasjen në të dhënat personale.

Jam i vetëdijshëm se çdo zbulim i paautorizuar i të dhënave personale në të cilat kam të drejtë të qasjes në kuadër të punës sime paraqet shkelje të detyrave të punës dhe etikës.

Për më shumë informacione **www.azlp.mk**

SCAN ME