Projekt – twining i BE-së „Mbështetje në zbatimin e kornizës së modernizuar ligjore për mbrojtjen e të dhënave personale”

UDHËZUES PËR OFICERË PËR MBROJTJEN E TË DHËNAVE PERSONALE NË SEKTORIN PUBLIK DHE PRIVAT

2022

Ky projekt financohet nga Bashkimi Evropian

LISTA E SHKURTESAVE DHE AKRONIMEVE

- **OMDHP** **Oficer për mbrojtjen e të dhënave personale**
- **LMDHP** **Ligji për mbrojtjen e të dhënave personale**
- **AMDHP** **Agjencia për Mbrojtjen e të Dhënave Personale**
- **GP29** **Grupi punues për nenin29 nga Direktiva 95/46**
- **BE** **Bashkimi Evropian**
- **KE** **Komisioni Evropian**
- **KEE** **Komuniteti Ekonomik Evropian**
- **GDPR** **Rregullativa e përgjithshme për mbrojtjen e të dhënave personale**

PËRMBAJTJA

Ky projekt financohet nga Bashkimi Evropian

Ky projekt financohet nga Bashkimi Evropian

KONCEPTI I PRIVATËSISË DHE MBROJTJA E TË DHËNAVE PERSONALE NË ERËN E DIGJITALIZIMIT

Kultura e respektimit të privatësisë dhe mbrojtja e të dhënave personale konsiderohet vlerë e madhe e shoqërive demokratike të cilat zhvillohen përmes zbatimit të standardeve bazë të vendosura nga Kombet e Bashkuara,[1]Këshilli i Evropës[2] dhe Komisioni Evropian[3], të cilat janë elaboruar në marrëveshjet ndërkombëtare dhe legjislacionin nacional për mbrojtjen e të dhënave personale.

Respektimi i të drejtës së privatësisë së personave fizikë është karakteristike për vendet më të zhvilluara me traditë të gjatë të sundimit të së drejtës dhe praktikave demokratike, por rëndësi e madhe i takon edhe respektimit të kësaj të drejte në mjediset shoqërore të cilat synojnëarritjen e nivelit më të lartë të jetës politike, juridike, ekonomike dhe kulturore.

Me miratimin e Ligjit për mbrojtjen e të dhënave personale (LMDHP)[4] e cila paraqet lex generalis në këtë fushë, Maqedonia e Veriut e inkoporon të drejtën për mbrojtjen e të dhënave personale në sistemin juridik në vend dhe futi koncept të ri i cili e thekson rëndësinë e kësaj të drejte si pjesë e të drejtave themelore dhe lirive të qytetarëve si dhe vlerë esenciale e çdo shoqërie të zhvilluar moderne dhe teknologjike.

Ky koncept nënkupton privatësinë dhe integritetin personal të të gjithë personave, në të gjitha situatat që përfshijnë përpunimin e të dhënave personale. Me rëndësi esenciale për realizimin e këtij koncepti dhe për vendosjen e standardeve më të larta për respektimin e privatësisë së kontrolluesve nga sektori publik dhe privat është të caktojnë oficer për mbrojtjen e të dhënave personale, së bashku me definicion të qartë të pozicionit të punës dhe kualifikimet e nevojshme për kryerësit e këtij funksioni, dhe ta intensifikojnë bashkëpunimin me Agjencinë për Mbrojtjen e të Dhënave personale (AMDHP).

[1] Kombet e Bashkuara, Konventa Evropiane për të Drejtat e Njeriut nga viti 1950
[2] Këshilli i Evropës, Konventa për Mbrojtjen e Personave Fizik në Raport të Përpunimit Automatik të të Dhënave Personale nr. 108/81.
[3] Komisioni Evropian, Direktiva 95/46 e Parlamentit Evropian dhe e Këshillit për Mbrojtjen e Personave Fizik në Raport të Përpunimit Automatik të të Dhënave Personale dhe lëvizjen e lirë të të dhënave të tilla,të miratuar më 24 tetor 1955, e cila nga 25 maji 2018 zëvendësohet me Rregullativën (EU) 2016/679 të Parlamentit Evropian dhe të Këshillit për Këshillit për Mbrojtjen e Personave Fizik në Raport të Përpunimit Automatik të të Dhënave Personale dhe lëvizjen e lirë të të dhënave të tilla me të cilën shfuqizohet Direktiva 95/46 , të miratuar më 27 prill 2016 (Rregullativa e Përgjithshme për Mbrojtjen e të Dhënave personale-GDPR).
[4] Ligji për mbrojtjen e të dhënave personale “Gazeta Zyrtare e Republikës së Maqedonisë së Veriut” nr. 42/20 dhe 294/21).

Ky projekt financohet nga Bashkimi Evropian

KUPTIMI DHE DEFINIMI I TERMEVE QË PËRDOREN NË UDHËZUES

Për qëllimet e përcaktimit të kuptimit të termeve që shfrytëzohen në këtë Udhëzues

Për qëllimet e përcaktimit të kuptimit të termeve që shfrytëzohen në këtë Udhëzues më poshtë janë dhënë definicione adekuate, ashtu siç ekzistojnë në Ligjin për mbrojtjen e të dhënave personale. Definimi i këtyre termeve i sqaron bazat mbi të cilat bazohet e drejta e mbrojtjes së të dhënave personale, e ndihmon kuptimin e esencës së ligjit dhe e lehtëson zbatimin.

.

E DHËNË PERSONALE është çdo informatë që ka të bëjë me person fizik të identifikuar ose person fizik i cili mund të identifikohet, kurse person fizik i cili mund të identifikohet është personi identiteti i të cilit mund të përcaktohet drejtpërsëdrejti ose tërthorazi, veçanërisht në bazë të identifikuesit siç janë emri/mbiemri, numri amë i qytetarit, të dhëna për lokacionin, identifikator nëpërmjet internetit, ose në bazë të një ose më shumë veçorive specifike për identitetin e tij fizik, fiziologjik, gjenetik, mental, ekonomik, kulturor ose social të atij personi fizik.

PËRPUNIM I TË DHËNAVE PERSONALE është çdo operacion ose përmbledhje e operacioneve të cilat kryhen mbi të dhënat personale, ose grup i të dhënave personale, në mënyrë automatike ose tjetër, siç janë: grumbullim, evidentim, organizim, strukturim, ruajtje, adaptim ose ndryshim, tërheqje, konsultim, këqyrje, përdorim, zbulim nëpërmjet transmetimit, publikim ose bërje të kapshme ndryshe, harmonizim ose kombinim, kufizim, shlyerje ose asgjësim.

SUBJEKT I TË DHËNAVE PERSONALE është çdo person fizik me të cilin kanë të bëjnë të dhënat personale të cilat përpunohen.

KONTROLLUES është personi fizik ose juridik, organi i pushtetit shtetëror, organi shtetëror ose personi juridik i themeluar nga shteti për kryerje të autorizimeve publike, agjencia ose trupi tjetër i cili në mënyrë të pavarur ose së bashku me të tjerë i përcakton qëllimet dhe mënyrën e përpunimit të të dhënave personale.

PËRPUNUES I PËRMBLEDHJES SË TË DHËNAVE PERSONALE është personi fizik ose juridik, organi i pushtetit shtetëror, organi shtetëror ose personi juridik i themeluar nga shteti për kryerje të autorizimeve publike, agjencia ose trupi tjetër që i përpunon të dhënat personale në emër të kontrolluesit.

OOFICER PËR MBROJTJEN E TË DHËNAVE PERSONALE është personi i autorizuar nga kontrolluesi që të sigurojë harmonizim me rregullativat për mbrojtjen e dhënave personale dhe ndjekjen e zbatimit të tyre.

PËLQIM I SUBJEKTIT TË TË DHËNAVE PERSONALE është çdo vullnet i paraqitur, i shprehur konkret, i informuar dhe i padyshimtë i subjektit të të dhënave personale nëpërmjet deklaratës ose veprimit qartë të konfirmuar, përmes të cilit shprehet pëlqimi për përpunimin e të dhënave personale të tij/saj për qëllime paraprakisht të përcaktuara.

KATEGORI TË VEÇANTA TË TË DHËNAVE PERSONALE (të dhëna të ndjeshme) janë të dhëna personale të cilat zbulojnë origjinë racore ose etnike, qëndrime politike, bindje fetare ose filozofike ose anëtarësi në organizata sindikale, si dhe të dhëna gjenetike, të dhëna biometrike, të dhëna që kanë të bëjnë me shëndetin ose të dhëna për jetën seksuale apo orientimin seksual të personit fizik.

cili është qëllimi i këtij udhëzuesi dhe kujt i dedikohet?

Ky udhëzues u dedikohet kontrolluesve dhe oficerëve për mbrojtjen e të dhënave personale të cilët janë përcaktuar nga kontrolluesit, në sektorin publik dhe privat.

Udhëzuesi ka për qëllim të sqarojë kuptimin e mbrojtjes të të dhënave personale dhe mënyrën në të cilën legjislacioni i ri i përfshin teknologjitë më të reja dhe zgjidhjet teknologjike kundrejt sfidave me të cilat ballafaqohet oficeri për mbrojtjen e të dhënave personale.

Qëllimet konkrete të Udhëzuesit janë që ta paraqesin rolin e oficerit për mbrojtjen e të dhënave personale, respektivisht:
ü t’i informojë për detyrat e tyre të cilat dalin nga legjislacioni nacional, respektivisht nga Ligji për mbrojtjen e të dhënave personale;
ü t’i sqarojë detyrimet ligjore të cilat kanë të bëjnë me përcaktimin e oficerit për mbrojtjen e të dhënave personale, si dhe dispozitat të cilat i definojnë kualifikimet e nevojshme për kryerjen e këtij pozicioni;

- t’i sqarojë detyrat e punës të oficerit për mbrojtjen e të dhënave personale, duke përfshirë edhe përgjegjësitë e kontrolluesit dhe përpunuesit të cilët janë të detyruar të përcaktojnë oficerë të tillë në kuadër të organizatës së tyre.

Udhëzuesi paraqet mjet të favorshëm praktik dhe arsimor për kontrolluesit dhe për oficerët për mbrojtjen e të dhënave personale përmes:
-sqarim të dispozitave relevante të GDPR të cilat janë të transponuara në legjislacionin nacional të Maqedonisë së Veriut;
-njohje të detajuar të oficerëve me rolin e tyre dhe detyrat e punës, si dhe të obligimet ligjore të kontrolluesve;
-dhënia e udhëzimeve për kontrolluesit/përpunuesit si t'i plotësojnë obligimet të cilat dalin nga LMDHP/GDPR, duke përfshirë edhe përmes përcaktimit të oficerit për mbrojtjen e të dhënave personale;
-rekomandime për praktika më të mira nga përvoja relevante në shtete-anëtare të Bashkimit Evropian (BE), por edhe nga praktika vendase; dhe

Ky dokument është organizuar në tri pjesë, me ç'rast PJESA 1 jep pasqyrë të dispozitave ligjore të cilat kanë të bëjnë në përcaktimin e oficerit për mbrojtjen e të dhënave personale si dhe kualifikimet e nevojshme për kryerësit e atij pozicioni të punës, PJESA 2 në mënyrë të detajuar i sqaron detyrat e punës së oficerit, obligimet e kontrolluesit dhe përpunuesit të cilat dalin nga legjislacioni i ri, si dhe pasqyrë e të drejtave të subjekteve të të dhënave personale, dhe PJESA 3 përfshin pako të mjeteve të cilat janë të favorshme për forcimin e pozicionit të oficerit për mbrojtjen e të dhënave personale.

PJESA 1: DETYRIME TË KONTROLLUESVE PËR CAKTIM TË OFICERIT PËR MBROJTJEN E TË DHËNAVE PERSONALE

Oficeri për mbrojtjen e të dhënave personale i balancon interesat e kontrolluesve dhe të përpunuesve me interesat e subjektit të dhënatpersonale të të cilit përpunohen, siguron plotësim të obligimeve të cilat dalin nga ligji, dhe janë pika e parë për kontakt me Agjencinë për Mbrojtjen e të Dhënave Personale (AMDHP).

Nga këtu, roli i këtyre oficerëve është specifik dhe unik, kurse pozicioni i tyre në kuadër të kontrolluesit duhet të jetë i rregulluar në mënyrë e cila e garanton pavarësinë dhe parandalon ndikime të mundshme politike ose ndikime tjera në kryerjen e detyrave të tyre.

Kjo pjesë nga Udhëzuesi mundohet të japë përgjigje në pyetjet si vijojnë
ü Cili është roli dhe detyrat e oficerit për mbrojtjen e të dhënave personale?
ü Cilat persona duhet të caktohen oficerë për mbrojtjen e të dhënave personale?
ü Çfarë aftësi dhe kualifikime duhet të posedojnë?
ü Si është rregulluar përcaktimi i oficerit për mbrojtjen e të dhënave personale në LMDHP?
ü Përcaktimi i detyrueshëm i oficerit për mbrojtjen të dhënave personale
üPërcaktimi vullnetar i oficerit për mbrojtjen të dhënave personale
üPërcaktimi vullnetar i oficerit për mbrojtjen të dhënave personale
üA mundet person i jashtëm të përcaktohet si oficer për mbrojtjen e të dhënave personale?
üNjë oficer për mbrojtjen e të dhënave personale për një ose më shumë kontrollues/përpunues
üCilat standarde profesionale duhet t’i plotësojë oficeri për mbrojtjen e të dhënave personale?
üPozicioni dhe statusi i oficerit për mbrojtjen e të dhënave personale.
üProfesionalizmi dhe aftësitë e oficerit për mbrojtjen e të dhënave personale.

- üPërfshirja e oficerit për mbrojtjen e të dhënave personale në çështjet lidhur me mbrojtjen e të dhënave personale.
- üGaranci për pavarësi të oficerit për mbrojtjen e të dhënave personale[1].
- üKonflikt interesi.
- üCaktimi dhe shkarkim të oficerit për mbrojtjen të dhënave personale.
- üRekomandim për kontrolluesit me madhësi të ndryshme të organizatës.

.

11. Cili është roli dhe detyrat e oficerit për mbrojtjen e të dhënave personale?

Detyrat e oficerit për mbrojtjen e të dhënave personale janë përcaktuar në nenin 43 nga Ligji për mbrojtjen e të dhënave personale dhe përfshijnë:
ü informim dhe këshillim të kontrolluesit ose përpunuesit dhe të punësuarve që kryejnë përpunimin e të dhënave personale për obligimet e tyre që dalin nga ligji;
ü ndjekje të harmonizimit të ligjit, me ligjet tjera relevant që merren me mbrojtjen e të dhënave personale në Republikën e Maqedonisë së Veriut, si dhe me politikat e kontrolluesit ose përpunuesit në lidhje me mbrojtjen e të dhënave personale, duke e përfshirë shpërndarjen e përgjegjësive të punës, ndërgjegjësimin dhe trajnimin e të punësuarve që do të kryejnë përpunim të të dhënave personale, si dhe në raport të zbatimit të revizioneve/kontrolle adekuate për mbrojtjen e të dhënave personale;
ü dhënie të këshillave kur është e nevojshme, në lidhje me vlerësimin e ndikimit të mbrojtjes së të dhënave personale dhe e ndjek kryerjen e vlerësimit në pajtim me nenin 39 të LMDHP-së;
ü bashkëpunon me Agjencinë;

- vepron si pikë kontakti për Agjencinë në lidhje me çështjet që kanë të bëjnë me përpunimin, duke e përfshirë konsultimin paraprak rregulluar në nenin 40 të LMDHP-së, si dhe këshillime/konsultime sipas nevojave për të gjitha çështjet tjera..

Oficerët duhet të hyjnë në komunikim të rregullt dhe bashkëpunim me AMDHP-në e cila përfshin përkrahje të Agjencisë për çështjet të cilat kanë të bëjnë me plotësimin e pozicionit të tyre, ndarjen e informacioneve të favorshme, etj. Bashkëpunimi i tillë u mundëson oficerëve për mbrojtjen e të dhënave personale harmonizim më të lehtë me dispozitat në këtë fushë.

Përveç kësaj, oficerët për mbrojtjen e të dhënave personale duhet të marrin pjesë në trajnimet që i organizon AMDHP të cilat nuk paraqesin vetëm mënyrë për përcaktimin dhe thellimin e njohurive të tyre, por edhe forma plotësuese për forcimin e bashkëpunimit me Agjencinë.

Cilat persona duhet të caktohenoficerË për mbrojtjen e të dhënave personale? Çfarë aftësi dhe kualifikime duhet të posedojnë?

Neni 41, paragrafi (5) nga LMDHP i përcakton kualifikimet profesionale të personave që përcaktohen oficerë për mbrojtjen e të dhënave personale, siç janë, për shembull, njohja e legjislacionit dhe praktikat për mbrojtjen e të dhënave personale, si dhe aftësi për plotësimin e detyrave të dhëna në nenin 43 nga LMDHP.

Konkretisht, oficer për mbrojtjen e të dhënave personale caktohet person i cili:
v i plotëson kushtet për punësim të përcaktuara në këtë ose ligj tjetër;
v në mënyrë aktive e shfrytëzon gjuhën maqedonase;
v në momentin e caktimit për oficer, të mos i jetë shqiptuar, me aktgjykim gjyqësor të plotfuqishëm dënim ose sanksion kundërvajtëse për ndalim për kryerjen e profesionit, veprimtarisë ose detyrës konkrete;
v ka mbaruar arsim të lartë;
v ka fituar njohuri dhe aftësi në raport të praktikave dhe dispozitave për mbrojtjene të dhënave personale në pajtim me dispozitat e LMDHP.

HNë nivel të Bashkimit Evropian, grupi punues për nenin (GP29) pranë Këshillit Evropian për mbrojtjen e të dhënave personale ka përgatitur “Udhëzime për oficer për mbrojtjen e të dhënave personale” [1], ku theksohet si vijon:
Ø oficeri për mbrojtjen e të dhënave personale duhet të ketë njohuri të mjaftueshme të operacioneve për përpunim që i kryen kontrolluesi (përkatësisht sektori adekuat dhe organizata), si dhe të sistemeve informatike, sigurinë e të dhënave dhe të nevojave për mbrojtjen e të dhënave personale;
Ø në rast të organit publik ose shtetëror, oficeri për mbrojtjen e të dhënave personale duhet të ketë njohuri solide në (internet) rregulla administrative dhe procedura në kuadër të organizatës.

1.2. si është rregulluar caktimi i oficerit për mbrojtjen e të dhënave personale në lmdhp?

Kontrolluesit dhe përpunuesit janë të detyruar të caktojnë oficer për mbrojtjen e të dhënave personale në të gjitha rastet ku:
1.përpunimin e të dhënave personale e kryen organi i administratës shtetërore, përveç gjykatave, por vetëm kur veprojnë në kuadër të kompetencave të tyre, por duhet të caktojnë oficer të tillë për të gjitha përpunimet tjera të të dhënave personale në pajtim me LMDHP;
2.veprimtarinë primare të kontrolluesit ose përpunuesit e përbëjnë operacione për përpunim të cilat, sipas natyrës , vëllimit dhe/ose qëllimit të tyre imponojnë ndjekje të rregullt dhe sistematike të subjektit të të dhënave personale nga përmasa të mëdha; ose
3.veprimtaria primare e kontrolluesit ose përpunuesit nënkupton përpunimin voluminoz të kategorive të posaçme të të dhënave personale ose të dhëna personale të cilat kanë të bëjnë me dënime penale ose vepra penale ashtu siç janë dhënë në nenin 14 të LMDHP.

Në pajtim me nenin 41, paragrafin 1 të LMDHP, detyrimi për caktim të detyrueshëm oficer për mbrojtjen e të dhënave personale ka të bëjnë me:

1.Të gjitha organet publike, me përjashtim të gjykatave vetëm kur veprojnë në kuadër të kompetencave të tyre; [1]

[1] Prapëseprapë, gjykatat janë të obliguara të caktojnë oficer për mbrojtjen e të dhënave personale e cila do të kujdeset për dispozitat për mbrojtjen e të dhënave personale në raport të operacioneve për përpunimin e të dhënave personale të cilat janë jashtë kompetencave të tyre gjyqësore.

1.kontrolluesit veprimtarinë primare të të cilëve e përbëjnë operacione për përpunim të cilat sipas natyrësvëllimit dhe/ose qëllimit të tyre imponojnë ndjekje të rregullt dhe sistematike të subjektit të të dhënave personale nga përmasa të mëdha; dhe
kontrolluesit/përpunuesit të cilët përpunojnë kategori të veçanta të të dhënave personale ose të dhëna personale lidhur me dënime penale dhe vepra penale.

GDPR nuk siguron definicion për atë që nënkuptohet nën veprimtari primare e cila përfshin ndjekje të rregullt dhe sistematike të subjektit të të dhënave personale, ose definicion për përpunim të të dhënave personale nga përmasa të mëdha.

Sqarimi i termeve

Megjithatë, Udhëzimet e përpunuara nga GP 29 në mënyrë më të detajuar i elaborojnë konceptet e lartpërmendura, respektivisht:
Øpër organet publike [1] duhet të konsiderohen edhe të gjitha kompanitë private me autorizime publike ose kompani të cilat kryejnë veprimtari me interes publik;

- rjedhimisht, organet shtetërore dhe publike përfshijnë pushtete nacionale, rajonale dhe lokale, por koncepti sipas ligjeve nacionale në fuqi, në mënyrë tipike përfshijnë edhe përfshirje të gjerë të trupave tjerë që e zbatojnë të drejtën publike. Në raste të tilla, përcaktimi i oficerit për mbrojtjen e të dhënave personale është i detyrueshëm pa marrë parasysh llojin dhevëllimin e të dhënave që përpunohen;

- veprimtari primare e kontrolluesit konsiderohen operacionet kryesore të cilat janë të nevojshme për arritjen e qëllimeve të kontrolluesit, me ç’rast veprimtaria primare nuk duhet të jetë vetëm ajo e cila ka të bëjë me përpunimin e të dhënave personale, por edhe aktivitete tjera të cilat rezultojnë me përpunimin e të dhënave personale;

  oshembull: dhënia e shërbimeve në fushën e komunikimeve elektronike, profilim, ndjekje e lokacionit përmes aplikacionit mobil, ndjekja e fitnes gjendjes dhe të dhëna për shëndetin përmes aplikacionit mobil, etj.

- Ø ndjekje sistematike dhe e rregullt e subjekteve të të dhënave personale përfshin të gjitha format e ndjekjes dhe profilim në internet, duke marrë parasysh faktin se termini për ndjekje nuk është kufizuar vetëm në mjedis onlajn;
-

  oshembull: dhënia e shërbimeve në fushën e komunikimeve elektronike, profilim, ndjekje e lokacionit përmes aplikacionit mobil, ndjekja e fitnes gjendjes dhe të dhëna për shëndetin përmes aplikacionit mobil, etj.

- Ø kur përcaktohet nëse bëhet fjalë për përpunimin nga përmasa të mëdha, GP 29 rekomandon që të merren parasysh faktorët si vijojnë:

  o numri i subjektit të të dhënave personale, si numër absolut ose si pjesë nga popullata relevante;
  o vëllimi i të dhënave personale që përpunohen dhe/ose përfshirja e pjesëve të ndryshme nga të dhënat personale;
  o kohëzgjatja, ose vazhdimësia e përpunimit të të dhënave personale;
  o distribuimi gjeografik i përpunimit të të dhënave personale.

Detyrimi për përcaktimin e oficerit për mbrojtjen e të dhënave personale ka të bëjë edhe me kontrolluesit edhe me përpunuesit.

1.2.2. CAKTIMI vullnetar i OFICERIT PËR MBROJTJEN E TË DHËNAVE PERSONALE

Edhe kur GDPR, respektivisht LMDHP nuk imponojnë përcaktim të detyrueshëm të oficerit për mbrojtjen e të dhënave personale, organizatat mund të konsiderojnë se është e favorshme të kenë oficer të tillë.

PГ29 inkurajon caktim vullnetar të oficerit për mbrojtjen e të dhënave personale.

Me këtë rast, kur ndonjë organizatë vullnetarisht cakton oficer për mbrojtjen e të dhënave personale që duhet të ketë parasysh se caktimi i tillë, duke përfshirë edhe pozicionin dhe detyrat e punës së oficerit i nënshtrohen plotësimit të dispozitave të dhëna në nenin 41 nga LMDHP njësoj sikur caktimi i tij/saj të kishte qenë detyrim ligjor.

Asgjë nuk pengon një organizatë e cila nuk është e obliguar ligjërisht të caktojnë oficer për mbrojtjen e të dhënave personale dhe nuk dëshiron vullnetarisht të caktojë oficer të tillë të ngarkojë ndonjë person të punësuar ose të angazhojë konsulent të jashtëm për kryerjen e detyrave të lidhura me mbrojtjen e të dhënave personale. Në rast të tillë, është e rëndësishme të shmanget çdo hamendje në lidhje me pozicionin e punës, statusin, pozitën dhe detyrat.

Nga këtu, komunikimi i përgjithshëm në kuadër të kompanisë, si dhe komunikim me organet për mbrojtjen e të dhënave personale, me subjektet e të dhënave personale, dhe me publikun, duhet qartë ta drejtojë faktin se pozicioni i punës i personit ose konsulenti nuk është oficer për mbrojtjen e të dhënave personale. Pa marrë parasysh nëse janë caktuar vullnetarisht ose në pajtim me detyrimin ligjor, oficeri për mbrojtjen e të dhënave personale janë të ngarkuar për të gjitha për përpunimin që i realizon kontrolluesi ose përpunuesi.

Me fjalë tjera, përveç nëse nuk është evidente qartë se kontrolluesi ose përpunuesi ka detyrim ligjor të caktojë oficer të tillë, GP29 rekomandon kontrolluesit ose përpunuesit të bëjnë analizë interne të faktorëve relevant dhe kriteret që të përcaktojë oficer për mbrojtjen e të dhënave personale ose jo. Kontrolluesit ose përpunuesit të cilët vullnetarisht kanë caktuar oficer për mbrojtjen e të dhënave personale kanë detyrime të njëjta si dhe kontrolluesit të cilët me ligj janë detyruar të caktojnë oficer.

1.2.3. A mundet person i jashtëm të caktohet si oficer për mbrojtjen e të dhënave personale?

Oficeri për mbrojtjen e të dhënave personale mund të jetë person i punësuar te kontrolluesi ose përpunuesi (oficer i brendshëm) ose detyrat e tilla mund t’i kryejë personi i angazhuar me kontratë në vepër

Në pajtim me Udhëzimet nga GP29, kjo do të thotë se personi i jashtëm mund të jetë oficer për mbrojtjen e të dhënave personale dhe në rast të tillë ky funksion mund të kryhet në bazë të marrëveshjes së lidhur mes personit dhe organizatës. Kur pozitën e oficerit për mbrojtjen e të dhënave personale e kryen person i jashtëm në bazë të kontratës në vepër, detyrat e punës mund të kryejë ekip i personave të cilat punojë për personin juridik të angazhuar, nën kryesim të personit fizik i cili është caktuar si lider i ekipit dhe përgjegjës për klientin konkret.

Në rast të tillë, me rëndësi esenciale është çdo anëtar jashtë organizatës i cili është angazhuar si oficer për mbrojtjen e të dhënave personalei plotëson kushtet adekuate të përcaktuara në LMDHP. Për qartësi më të madhe juridike dhe organizim të mirë, si dhe për parandalim konflikt interesi mes anëtarëve të ekipit, Udhëzimet e GP29 rekomandojnë marrëveshja të përfshijnë shpërndarje të detyrave të punës në kuadër të ekipit të jashtëm i cili vepron si oficer për mbrojtjen e të dhënave personale dhe përcaktim lider të ekipit i cili është përgjegjës për klientin.

Në të njëjtën kohë, është e mundshme kombinimi i aftësive individuale dhe anët e fuqishme me qëllim disa persona, të cilët punojnë si ekip, në mënyrë efikase të mund të shërbejnë klientët e tyre.

1.2.4. Një oficer për mbrojtjen e të dhënave personale për një ose më shumë kontrollues/përpunues

Udhëzimet e GP29 japin mundësi për caktimin e një oficeri për mbrojtjen e të dhënave personale i cili shërben më shumë kontrollues/përpunues, dhe atë në rastet si vijojnë:

- Ø SEKTORI PRIVAT: kompani më të vogla të cilat punojnë së bashku si grupacion i caktuar mund të caktojnë një oficer;[1].

- Ø SEKTORI PUBLIK: duke pasur parasysh strukturën e tyre organizative dhe madhësinë, më shumë shtete dhe organe tjera mund të caktojnë oficer për mbrojtjen e të dhënave personale.[1] Gjithashtu, ky oficer mund të jetë i angazhuar në bazë të marrëveshjes në vepër për sigurimin e shërbimit të tillë.

[1] Personi mund të jetë angazhuar me kontratë për sigurim të shërbimit.

Në pajtim me Udhëzimet e GP29 oficeri për mbrojtjen e të dhënave personale, duhet të jetë i arritshëm për subjektet e të dhënave personale, organin mbikëqyrës (AMDHP), dhe duhet të jetë i arritshëm për të punësuarit në kuadër të kontrolluesit ose përpunuesit. Sqarimi për qasjen te oficeri për mbrojtjen e të dhënave personale i cili është përcaktuar për më shumë kontrollues ka të bëjë edhe me sektorin publik edhe me atë privat.

Që të sigurohet se oficeri për mbrojtjen e të dhënave personale është i arritshëm, pa marrë parasysh nëse bëhet fjalë për person të brendshëm ose të jashtëm, është me rëndësi që kontakt detajet e tij të shpallen dhe të ndahen në publik. Oficeri, me ndihmë të ekipit kur ajo është e nevojshme, duhet të jetë në pozitë në mënyrë efektive të komunikojë me subjektet e të dhënave personale dhe të bashkëpunojë me organin mbikëqyrës. Mes tjerash, kjo do të thotë se komunikimi duhet të zhvillohet në gjuhën/gjuhët që i shfrytëzon AMDHP-ja dhe subjektet e prekura të të dhënave personale. Qasja te oficeri, pa marrë parasysh nëse bëhet fjalë për qasje fizike në kuadër të hapësirave afariste, përmes internetit ose përmes ndonjë mjeti tjetër të sigurt për komunikim, është me rëndësi esenciale që të sigurohet se subjektet e të dhënave personale mund ta kontaktojnë atë.

Detyrimi për publikim të kontakt detaleve të oficerit

Neni 41 , paragrafi (7) nga LMDHP përcakton se kontrolluesi ose përpunuesi publikisht i publikon kontakt detalet e oficerit për mbrojtjen e të dhënave personale dhe e njofton Agjencinë.

Qëllimi është sigurimi i kontaktit të lehtë dhe direkt dhe komunikimit mes oficerit dhe subjektit të të dhënave personale dhe organit mbikëqyrës. Kontakt detalet e oficerit duhet të përfshijnë informacionet si vijojnë: Numër telefoni dhe posta elektronike, si dhe forma të posaçme për kontakt të ueb faqes të kontrolluesit. Kjo dispozitë na udhëzon në nevojën për theksim të emrit personal të oficerit për mbrojtjen e të dhënave personale si pjesë nga kontakt detalet e tij/saj.[1]

GP29 rekomandon organi mbikëqyrës (AMDHP) të jetë i informuar për emrin dhe kontakt detalet e oficerit për mbrojtjen e të dhënave personale dhe të njëjtat do të publikohen në ueb faqen e kontrolluesit/përpunuesit, në listën telefonike interne ose si pjesë e organogramit.

Detyrimi për fshehtësi dhe besueshmëri të të dhënave

Përveç kësaj, oficeri për mbrojtjen e të dhënave personale ka për detyrë për fshehtësi dhe besueshmëri gjatë kryerjes së detyrave të tij/saj, në të njëjtën kohë nuk i nënshtrohet në ndalimin për kontaktim me dhe kërkim i këshillave nga organi mbikëqyrës (AMDHP).

1.3. Cilat standarde profesionale duhet t’i plotësojë oficeri për mbrojtjen e të dhënave personale?

Me legjislacionin e ri oficeri për mbrojtjen e të dhënave personale merr pozitë të pavarur strategjike që të sigurojë efektivitet më të madh në realizimin e këtij pozicioni të punës dhe nivel më të lartë të mbrojtjes të të dhënave personale.

Ligji i ri përcakton se oficeri për mbrojtjen e të dhënave personale duhet t’i posedojë kualifikimet profesionale, njohuritë profesionale për dispozitat dhe praktikat, dhe aftësitë për moskryerje të detyrave të punës si dhe të marrë garanci nga udhëheqësi i kontrolluesit për kryerje të pavarur të detyrave të tij/saj.

Ky udhëzues i definon të gjitha standardet profesionale që duhet t’i plotësojnë kandidatët për oficer për mbrojtjen e të dhënave personale, ashtu siç është përcaktuar në LMDHP.

Qëllimi kryesor i standardeve të tilla profesionale është:

Ø përcaktimi i profilit të personalit profesional dhe ekspert i cili emërohet si oficer për mbrojtjen e të dhënave personale;
Ø definimi i standardeve minimale lidhur me pozicionin oficer për mbrojtjen e të dhënave personale të cilat duhet të jenë të dizajnuara në mënyrë e cila e siguron pavarësinë e tyre/saj.

Gjatë caktimit të oficerit për mbrojtjen e të dhënave personale rekomandohet kontrolluesit t'i zbatojnë standardet profesionale (kushte) të definuara më poshtë.

KUSHTET PËR CAKTIM TË OFICERIT PËR MBROJTJEN TË DHËNAVE PERSONALE

Neni 41, paragrafi (5) nga LMDHP përcakton se oficeri për mbrojtjen e të dhënave personale përcaktohet në bazë të kualifikimeve të tij/saj profesionale, kurse në bazë të njohurive të ligjit dhe praktikave në fushën e mbrojtjes së të dhënave personale dhe aftësive për t'i kryer detyrat e theksuara në nenin 43 nga LMDHP.

Kërkesat profesionale:
-t'i plotësojnë kushtet për punësim të përcaktuara në LMDHP ose ligj tjetër;
-në mënyrë aktive ta përdorë gjuhën maqedonase;
-në momentin e përcaktimit, me aktvendim të plotfuqishëm nuk i është shqiptuar dënim ose sanksion kundërvajtës ndalim për kryerjen e profesionit, veprimtarisë ose detyrës;
-të ketë mbaruar arsim të lartë;
-të ketë fituar njohuri dhe aftësi lidhur me praktikat dhe dispozitat për mbrojtjen e të dhënave personale në pajtim me dispozitat nga LMDHP.

Kualitetet personale:

- Ø Aftësi personale: integritet, iniciativë, organizim, diskrecion, qëndrueshmëri, interes dhe motivim për kryerjen e këtij funksioni, si dhe nivel i lartë i etikës profesionale, zhvillmi i aftësive dhe zbatimin e praktikave konkrete me imponim të ndryshimit kur ajo është e nevojshme, dhe aftësia për kryerjen dhe bartjen e njohurive dhe pozicion i qartë, si dhe afirmim personal i pozicionit kur është e nevojshme;
- Ø aftësi interpersonale: komunikim, aftësi për negociata dhe zgjedhje të konflikteve.

CERTIFIKATAT E OFICERIT PËR MBROJTJEN E TË DHËNAVE PERSONALE, MIRËMBAJTJA DHE PËRSOSJA E NJOHURIVE PROFESIONALE

Detyrimi ligjor për certifikim

- Ø Lëshimi i certifikatës për trajnim të mbaruar për oficer për mbrojtjen e të dhënave personale si provë për njohuri profesionale të fituara për dispozitat dhe praktikat në këtë fushë si kusht për përcaktim të pozicionit oficer për mbrojtjen e të dhënave personale.
-

Detyrimi ligjor për mirëmbajtje dhe përsosje të njohurive profesionale
Pas emërimit të pozicionit të punës, oficeri për mbrojtjen e të dhënave personale duhet:
Ø t'i ndjekë rregullisht trajnimet që i organizon AMDHP, si dhe trajnimet e certifikuara që i organizojnë dhënësit tjerë të shërbimeve të cilët janë akreditуar për organizimin dhe kryerjen e trajnimeve (organizime profesionale), si vendase ashtu edhe nga shtete anëtare të BE-së;
Ø të inkorporojnë forma të reja të trajnimit si mënyrë për vetë përmirësim përmes rrjetit të oficerëve.

1.4. Pozicioni dhe statusi i oficerit për mbrojtjen e të dhënave personale.

1.4.1. profesionalizmI dhe aftësiA

Kontrolluesit janë përgjegjës që të sigurojnë zbatim dhe të demonstrojnë harmonizim me dispozitat për mbrojtjen e të dhënave personale, me ç'rast oficeri për mbrojtjen e të dhënave personale është figura kryesore përmes të cilës kontrolluesi e plotëson këtë detyrim.

Sipas nenit 42 nga LMDHP, kontrolluesi dhe përpunuesi janë të detyruar të sigurojnë se oficeri për mbrojtjen e të dhënave personale në mënyrë adekuate dhe në kohë është i përfshirë në të gjitha çështjet lidhur me mbrojtjen e të dhënave personale.

Përveç kësaj, kontrolluesi dhe përpunuesi janë të detyruar të sigurojnë përkrahje të oficerit për mbrojtjen e të dhënave personale gjatë kryerjes së detyrave të punës të theksuara në nenin 43 nga LMDHP, përmes sigurimit të resurseve të cilat janë të domosdoshme për kryerjen e atyre detyrave dhe qasjes te të dhënat personale dhe operacioneve për punë, dhe përmes mbajtjes së njohurive profesionale të tij/saj.

Subjektet e të dhënave personale mund ta kontaktojnë oficerin për mbrojtjen e të dhënave personale për të gjitha çështjet lidhur me përpunimin e të dhënave të tyre personale dhe për realizimin e të drejtave që i takojnë në pajtim me LMDHP.

Sipas GDPR, respektivisht LMDHP, oficeri për mbrojtjen e të dhënave personale duhet të jetë i pavarur në kuadër të organizatës. Zgjidhja e re ligjore është përpunuar në mënyrë e cila siguron pavarësi të oficerit ose kryerjen e atij pozicioni pa ndonjë ndikim dhe instruksion.

Megjithatë, pavarësia e oficerit për mbrojtjen e të dhënave personale nuk do të thotë se kryerësi i këtij funksioni ka autorizim për miratimin e vendimeve sepse ajo do thoshte tejkalim i detyrave dhe angazhimeve të tij/saj.

Fakti se oficeri për mbrojtjen e të dhënave personale është pjesë nga kontrolluesi jep mundësi ideale për sigurim të harmonizimit me dispozitat për mbrojtjen e të dhënave personale nga brenda, përmes dhënies së këshillave ose intervenimit në raste kur ajo është e nevojshme që të shmangen aksione ngaAMDHP.

Nëse kontrolluesi miraton vendim që është jokompatibil me rregullat dhe me këshillën nga oficeri, atëherë oficeri për mbrojtjen e të dhënave personale duhet të jenë në mundësi për mendim të ndarë.

1.4.2. përfshirja e oficerit për mbrojtjen e të dhënave personale në të gjitha çështjet lidhur me mbrojtjen e të dhënave personale

Oficeri për mbrojtjen e të dhënave personale në mënyrë adekuate dhe në kohë duhet të jetë i kyçur (që në fazat e hershme) në të gjitha çështjet e lidhura me mbrojtjen e të dhënave personale.

1.4.3. GaranciTË për pavarësi të oficerit për mbrojtjen e të dhënave personale

Neni 42, paragrafi (2) nga LMDHP përcakton se kontrolluesi dhe përpunuesi duhet të sigurojnë se oficeri për mbrojtjen e të dhënave personale nuk merr asnjë instruksion në raport të kryerjes të detyrave të punëve të tij/saj.

Neni 42, paragrafi (3) nga LMDHP vendos garanci të caktuara bazike që u ndihmojnë oficerëve për mbrojtjen e të dhënave personale të jenë në mundësi të kryejnë detyrat e tyre të punës me nivel të konsiderueshëm të pavarësisë në kuadër të organizatës. Shënim sqarues nr. 97 (recital) drejt GDPR shtohet se “pa marrë parasysh nëse janë të punësuar personat te kontrolluesi ose jo, oficerët për mbrojtjen e të dhënave personale duhet të jenë në pozicion t’i kryejnë detyrat e tyre të punës në mënyrë të pavarur".

Udhëzimet e GP29 sqarojnë se oficerët nuk guxojnë të marrin instruksione si të ballafaqohen me disa gjëra, për shembull, cilat rezultate duhet të arrihen, si të hetohet ndonjë ankesë, ose nëse do të konsultohet me organin mbikëqyrës.

Kontrolluesi dhe përpunuesi mbeten përgjegjës për harmonizim me Ligjin për mbrojtjen e të dhënave personale dhe duhet ta demonstrojnë këtë.

Nëse kontrolluesi ose përpunuesi miratojnë vendime të cilat janë jokompatibile me GDPR/LMDHP dhe me këshillën nga oficeri, atëherë oficeri për mbrojtjen e të dhënave personale duhet të jetë në mundësi të japë mendim të ndarë te niveli udhëheqës më i lartë dhe te personat që miratojnë vendime.

1.4.4. konflikti i interesiave

Neni 42, paragrafi (6) nga LMDHP përcakton se oficeri për mbrojtjen të dhënave personale mund të kryejë edhe punë dhe detyra tjera. Kontrolluesit dhe përpunuesit janë të detyruar të sigurojnë detyra dhe angazhime të tilla që nuk çojnë në konflikt të interesave.

Mungesa e konfliktit të interesave është e lidhur ngushtë me kërkesën për kryerje të pavarur të funksionit. Edhe pse oficerëve për mbrojtjen e të dhënave personale u është lejuar të kryejnë edhe detyra dhe angazhime tjera, ngarkimet e tilla nuk duhet të çojnë në konflikt të interesave.

Sipas Udhëzimit të GP29 ajo në veçanti ka të bëjë në faktin se oficeri për mbrojtjen e të dhënave personale nuk mund t'i kryejnë pozicionet në kuadër të organizatës e cila mund të sjellë në situatë t'i përcaktojë qëllimet dhe mjetet për përpunim të të dhënave personale. Për shkak të strukturës organizative specifike të një organizate, kjo dispozitë duhet të shqyrtohet në bazën nga rasti - në rast.

Në pajtim me praktikat pozitive, pozicionet në kuadër të organizatës të cilat mund të jenë në konflikt me këtë rregull përfshijnë pozicione udhëheqëse të larta (për shembull, drejtor ekzekutiv, drejtor operativ, drejtor financiar, udhëheqës i seksionit për marketing, udhëheqës i seksionit për resurse njerëzore, ose udhëheqës i seksionit për teknologji informatike), por edhe pozicione tjera më të ulëta në kuadër të strukturës organizative nëse të njëjtat nënkuptojnë përcaktim të qëllimeve dhe mjeteve për përpunim të të dhënave personale.

Përveç kësaj, konflikti i interesave mund të paraqitet, për shembull, nëse nga oficeri për mbrojtjen e të dhënave personale i angazhuar nga jashtë kërkohet ta përfaqësojë kontrolluesin ose përpunuesin para gjykatës në lëndë e cila përfshin çështje lidhur me mbrojtjen e të dhënave personale.

Në varësi të veprimtarisë, madhësia e strukturës së organizatës, praktika të mira për kontrolluesit ose përpunuesit përfshijnë:
·identifikim të pozicioneve të punës të cilat janë jokompatibile me detyrat e punës të oficerit për mbrojtjen e të dhënave personale;
·përgatitje të rregullave interne për parandalim të konfliktit të interesit;
· sigurim të sqarimit më të përgjithshëm për konflikt të interesit;

·deponim të deklaratës se oficeri për mbrojtjen e të dhënave personale nuk ka konflikt të interesit në raport të kryerjes së atij funksioni si mënyrë për ndërtim të vetëdijes për këtë kusht;
· vendosje të masave mbrojtëse në rregullat interne të organizatës që të sigurohet se shpallja për plotësim të pozicionit të punës oficer për mbrojtjen e të dhënave personale ose marrëveshja në vepër për atë funksion janë mjaft precize dhe të detajuara që të shmanget konflikt i interesave.

Në këtë kontekst, duhet të kihet parasysh se konflikti i interesave mund të ketë formë të ndryshme në varësi të asaj nëse oficeri është angazhuar nga rangu i të punësuarve ose si person i jashtëm.

1.5. Caktimi dhe shkarkimi i oficerit për mbrojtjen të dhënave personale

Sipas nenit 42 nga LMDHP, oficeri për mbrojtjen e të dhënave personale nuk mund të jenë të përjashtuar nga vendi i punës ose të dënuar nga kontrolluesi ose përpunuesi për kryerjen e detyrave të punës së tyre. Oficeri për mbrojtjen e të dhënave personale drejtpërdrejtë përgjigjet para nivelit më të lartë udhëheqës të kontrolluesit ose përpunuesit.

Disa praktika të mira të cilat sigurojnë harmonizim të kontrollorëve dhe përpunuesve me kërkesat e përcaktuara në nenin 42 nga LMDHP përfshijnë:

Caktim/ shkarkim

- Ø Caktim të bartësit të funksionit oficer për mbrojtjen e të dhënave personale për kohë të papërcaktuar ose për aq kohë sa më të gjatë tëmundshme ;
- Ø Dorëzim të informatave për kontakt për oficerin e caktuar për mbrojtjen e të dhënave personale deri te AMDHP;
- Ø Revokim/shkarkim të bartësit të funksionit oficer për mbrojtjen e të dhënave personale vetëm nëse personi më nuk i plotëson kushtet për kryerjen e detyrave të punës dhe angazhimet;
-

Resurse njerëzore dhe resurse tjera

- Ø Sigurim të resurseve të nevojshme njerëzore dhe resurseve tjera për kryerjen e detyrave të punës, duke përfshirë edhe qasje tek operacionet për përpunim të të dhënave personale, si dhe mundësimi dhe avancimi i njohurive profesionale të oficerit për mbrojtjen e të dhënave personale;
- Ø përpunim të planit të punës për vlerësim të nevojave për resurse njerëzore dhe resurse tjera;
- Ø përkrahje aktive nga niveli më i lartë i punës në raport të sigurimit të personelit të nevojshëm, resurseve financiare dhe infrastrukturës të cilat janë të domosdoshme për pozicionin oficer për mbrojtjen e të dhënave personale;

Lirimi nga detyra tjera të punës dhe angazhime

- Ø lirim adekuat i oficerit për mbrojtjen e të dhënave personale nga detyrat dhe angazhimet tjera me qëllim të fokusohet në detyrat të cilat janë lidhur me kryerjen e këtij funksioni;

Struktura e brendshme adekuate në kuadër të kontrolluesit

- Ø Organizim adekuat i strukturës së brendshme sipas të cilës oficeri për mbrojtjen e të dhënave personale udhëheq me seksionin për mbrojtjen e të dhënave personale (nëse është vendosur), ose e kryen atë funksion si person i pavarur në nivel adekuat në kuadër të hierarkisë së kontrolluesit i cili garanton veprim të pavarur, respektivisht udhëheqje të këtij funksioni në mënyrë që pengon çfarëdo ndikimi ose marrjen e instruksioneve për kryerjen e detyrave të punës;
- Ø përjashtim të mundësisë për revokim ose dënim të bartësit të funksionit oficer për mbrojtjen e të dhënave personale për shkak të kryerjes së detyrave të punës të tij/saj.
-

Rregullimi i bashkëpunimit me nivelin më të lartë udhëheqës si pjesë nga dispozitat interne

- Ø Informimi i nivelit më të lartë udhëheqës vlen për çështjet nga fusha e mbrojtjes së të dhënave personale, në masë më të vogël çdo tre muaj, dhe mbajtjen e takimeve tematike kur ajo është e nevojshme;
- Ø përgjegjësi direkte e oficerit për mbrojtjen e të dhënave personale para nivelit më të lartë udhëheqës
- Ø sigurimi i shikueshmërisë së funksionit oficer për mbrojtjen e të dhënave personale në kuadër të strukturës organizative;
- Ø rregullimi i detyrimit për të gjithë të punësuarit të bashkëpunojnë me oficerin për mbrojtjen e të dhënave personale pa kërkuar paraprakisht leje për atë nga eprorët e tyre;
- Ø miratimi i dispozitave interne të cilat i rregullojnë rastet e konsultimit të detyrueshëm me oficerin për mbrojtjen e të dhënave personale;
- Ø Autorizim i oficerit për mbrojtjen e të dhënave personale ta parafojnë korrespodencën e cila ka të bëjë me mbrojtjen e të dhënave personale;
- Ø caktimi i zëvendësoficerit për mbrojtjen e të dhënave personale që të sigurohet vazhdimësi në kryerjen e këtij funksioni në rast të mungesës së oficerit, me ç’rast duhet t’i ketë kufijtë e njëjtë për kryerje të pavarur të funksionit të tij/saj;

Rregullimi i zbatimit të revizioneve/kontrolleve/shqyrtimeve

- Ø Miratimi i rregullave të detajuara për zbatimin e revizioneve/kontrolleve/shqyrtimeve nga ana e oficerit për mbrojtjen e të dhënave personale;
- Ø Mundësimi i qasjes së oficerit për mbrojtjen e të dhënave personale te hapësirat dhe sistemet kur kryen operacionet për përpunim, dhe vendosjen e detyrimit për komunikim me personat të cilët kanë parashtruar ankesë për shkelje të legjislacionit në fushën e mbrojtjes së të dhënave personale;

ELEMENTET QË E DOBËSOJNË POZICIONIN E OFICERIT PËR MBROJTJEN E TË DHËNAVE PERSONALE

Nëse oficeri kryen edhe detyra tjera të punës në mënyrë plotësuese nga ato lidhur me funksionin e tij, ai/ajo mund të ballafaqohet me konflikt në raport të kohës të kaluar në kryerjen e detyrave të cilat nuk janë lidhur drejtpërdrejt me funksionin e tij/saj dhe qëllimin e kryerjes së detyrave lidhur me mbrojtjen e të dhënave personale. Nga këtu, në situata ku supozimet japin peshë të madhe në detyrat tjera ajo mund të krijojë presion mbi oficerin për mbrojtjen e të dhënave personale të fokusohet në detyrat e tij dhe mund të çojë në kryerje joefikase të detyrave lidhur me funksionin e tij/saj. Përveç kësaj, ekziston besueshmëri e madhe detyrat e tilla të çojnë në konflikt të interesit.

Kur oficeri për mbrojtjen e të dhënave personale ka marrëveshje për punë në kohë të caktuar, ai/ajo është vënë në pozitë të pavolitshme dhe sigurisht do të shfaqë përkushtim dhe mund më të vogël në kryerjen e detyrave të punës për dallim nga oficer që ka marrëveshje për punë në kohë të pacaktuar për shkak të brengosjes nëse marrëveshja për punë do të vazhdohet ose jo.

Sigurisht që oficerët të cilët janë përgjegjës në mënyrë të drejtpërdrejtë ose janë nën kontroll të eprorit mund të ndjejnë presion, me ç’rast kryerja e tyre e pavarur e këtij funksioni mund të ndikojë negativisht mbi avancimin në karrierë. Përkatësisht, kryerja korrekte dhe adekuate e detyrave të punës të oficerit për mbrojtjen e të dhënave personale shpesh herë imponon të marrin qëndrim të fortë i cili është në kundërt të eprorëve dhe të kërkojnë plotësimin e obligimeve të cilat kanë funksione më të larta në kuadër të kontrolluesit, dhe nga këto arsye mund të jenë të perceptuara si "burokrat” ose “ krijues të problemeve”. Oficeri për mbrojtjen e të dhënave personale duhet të ketë status të pavarur që i ndihmon t’i qëndrojnë presioneve dhe pengesave të cilat janë të lidhura me këtë funksion të rëndësishëm. Nga këtu, që të lehtësohet presioni i tillë, oficeri duhet të jetë direkt përgjegjës para nivelit më të lartë udhëheqës në kuadër të kontrolluesit.

Oficerët për mbrojtjen e të dhënave personale të cilat janë në pozitë të kërkojnë resurse njerëzore dhe resurse tjera nga persona eprorë të drejtpërdrejtë mund të ballafaqohen me pengesa nëse personat eprorë nuk janë tërësisht të përkushtuar në arritjen e harmonizimit me dispozitat për mbrojtjen e të dhënave personale. Situata e tillë mund të shmanget nëse oficeri ka buxhet personal dhe kërkesat e tij/saj janë lëndë e miratimit nga ana e nivelit më të lartë udhëheqës në kuadër të kontrolluesit.

1.6. RekomandimE për kontrolluesit me madhësi të ndryshme të organizatës

Kriteret për kategorizim

Përcaktimi i kritereve për kategorizim të kontrolluesve në varësi të madhësisë së tyre është i rëndë sepse ekzistojnë kontrollues me numër të vogël të të punësuarve, por numër të madh të operacioneve për përpunim të të dhënave personale ose përpunim të kategorive të posaçme të të dhënave personale dhe e anasjelltas, ekzistojnë kontrollues me numër të madh të të punësuarve të cilët kryejnë përpunim të të dhënave personale përveç asaj lidhur me të dhënat personale të të punësuarve të tyre.

Nga këto arsye, është vështirë të përcaktohet numër i vogël i obligimeve lidhur me kryerjen e funksionit oficer për mbrojtjen e të dhënave personale te kontrolluesit më të vegjël kundrejt atyre më të mëdhenj.

Nga ana tjetër, fakt është se kontrolluesit më të vegjël nuk kanë mjaftueshëm resurse financiare dhe njerëzore që t'i plotësojnë detyrimet ligjore lidhur me kryerjen e këtij funksioni.

Kontrollues të vegjël

- Ø një oficer për mbrojtjen e të dhënave personale mund të caktohet për më shumë kontrollues të vegjël të cilët punojnë si grup i kontrolluesve ose të cilët nuk kanë strukturë të komplikuar organizative;
- Ø oficeri për mbrojtje mund të angazhohet me kontratë në vepër;
- Ø në rast kur oficeri kryen edhe detyra tjera, kontrolluesit duhet të sigurojnë garanci se nuk ekziston konflikt interesash me funksionin e tyre primar;

Ky projekt financohet nga Bashkimi Evropian

Kontrollues të mëdhenj

- Ø përcaktimi i pozicionit oficer për mbrojtjen e të dhënave personale si vend pune me kohë të plotë të punës, që do të thotë lirim të kryerësit të funksionit nga detyra tjera të punës dhe angazhime që të mund të përkushtohet në detyrat e punës lidhur me mbrojtjen e të dhënave personale;
- Ø sigurimi i resurseve të nevojshme njerëzore dhe resurseve tjera për oficerin për mbrojtjen e të dhënave personale që të mund t’i kryejnë detyrat e punës. Kur vëllimi i punës e imponon këtë, kontrolluesi duhet të formojë ekip, të udhëhequr nga oficeri, për kryerjen e detyrave të punës lidhur me mbrojtjen e të dhënave personale. Struktura e brendshme e ekipit, si dhe detyrat dhe përgjegjësitë e çdo anëtari të ekipit, duhet të jenë të definuara qartë.
- Ø Zbatimi i vlerësimit të ndikimit mbi mbrojtjen e të dhënave personale në lidhje me operacionet e planifikuara për përpunim, kur procesi i tillë nuk është vendosur paraprakisht në kuadërtë kontrolluesit.
-

PJESA 2: Roli i oficerit për mbrojtjen e të dhënave personale

Kjo pjesë nga Udhëzuesi në mënyrë të detajuar i elaboron detyrat e oficerit për mbrojtjen e të dhënave personale, ashtu siç është rregulluar në Ligjin për mbrojtjen e të dhënave personale.

2. informimi dhe vePRIMI sipas kërkesAVE për mbrojtjen e të drejtave të subjektit të të dhënave personale

Oficeri për mbrojtjen e të dhënave personale është i detyruar t’i informojë subjektet e të dhënave personale për të drejtat e tyre, por në të njëjtën kohë edhe ta këshillojë kontrolluesin për detyrimet e tij të cilat dalin nga dispozitat për mbrojtjen e të dhënave personale.

2.1. të drejtat e subjektit të të dhënave personale

Subjektet e të dhënave personale në pajtim me Ligjin për mbrojtjen e të dhënave personale i kanë të drejtat si vijojnë:

- ü E drejta e informimit
- ü E drejta e qasjes te të dhënat personale
- ü E drejta e korrigjimit
- ü E drejta e shlyerjes (“ e drejta të jesh i harruar”)
- ü E drejta e kufizimit të përpunimit
- ü E drejta e bartjes së të dhënave
- ü E drejta e ankesës
- ü E drejta për të mos qenë lëndë e miratimit të automatizuar të vendimeve individuale duke përfshirë edhe profilimin

Më shumë për të drejta të subjektit mund të lexoni në Informatorin me temë Të drejtat e qytetarëve si subjekte të të dhënave personale i arritshëm në linkun si vijon link .

Kërkesa për ndryshim, modifikim dhe shlyerje ose ndërprerje të përpunimit të të dhënave personale.

Me kërkesë të subjektit të të dhënave personale, kontrolluesi është i detyruar t'i plotësojë, ndryshojë dhe shlyejë të dhënat personale ose ta ndërpresë përpunimin e të dhënave personale në raste kur janë të paplota, të pasakta ose të parashkruara, ose në rast të përpunimit joligjor.

Pa marrë parasysh faktin nëse subjekti i të dhënave personale ka parashtruar kërkesë, kur ka përcaktuar se të dhënat personale janë të paplota, të pasakta ose të parashkruara, kontrolluesi është i obliguar t'i plotësojë, ndryshojë ose shlyejë.

Në afat prej 30 ditëve pas pranimit të kërkesës, kontrolluesi është i obliguar ta njoftojë subjektin e të dhënave personale për plotësim, ndryshim ose shlyerje të të dhënave personale.

Në këtë kontekst, oficeri për mbrojtjen e të dhënave personale është i detyrueshëm për realizim të të drejtave të subjektit të të dhënave personale dhe për plotësim të detyrimeve të kontrolluesit.

2.2. obligimi i kontrolluesit/përpunuesit

2.2.1. respektimi i parimit për mbrojtjen e të dhënave personale

Kontrolluesit janë të detyruar të veprojnë në pajtim me parimin për mbrojtjen e të dhënave personale.

- **Ø Ligjshmëri, drejtësi dhe transparencë**

Çdo përpunim i të dhënave personale duhet të jetë ligjor dhe i drejtë. Në të njëjtën kohë, duhet të jetë transparent, që do të thotë se personat fizikë ë duhet të jenë të informuar për grumbullimin, shfrytëzimin, konsultimin dhe ndonjë tjetër përpunim të të dhënave të tyre personale, si dhe shkallën deri te e cila të dhënat përpunohen ose do të përpunohen. Parimi i transparencës imponon informatat dhe komunikimi në lidhje me përpunimin e të dhënave personale të jenë lehtë të arritshme dhe të kuptueshme, respektivisht të jenë të dhëna në gjuhë të qartë dhe të thjeshtë.

- **Ø Kufizimi i qëllimeve**

Të dhënat personale duhet të grumbullohen vetëm për qëllime konkrete të qarta dhe legjitime dhe ato nuk guxojnë të jenë lëndë e përpunimit të mëtejshëm në mënyrë e cila nuk është në pajtim me ato qëllime. Megjithatë, përpunimi i mëtejshëm i të dhënave personale për qëllime të arkivimit është interes publik, për hulumtime historike dhe shkencore dhe për qëllime statistikore në pajtim me nenin 86, paragrafin (2) nga LMDHP, nuk konsiderohet për jokompatibil me qëllim inicial të përpunimit.

- **Ø Vëllimi minimal i të dhënave**

Përpunimi i të dhënave personale duhet të jetë adekuat, relevant dhe i kufizuar vetëm në atë që është e domosdoshme për arritjen e qëllimeve për përpunim të tillë. Të dhënat personale duhet të përpunohen vetëm nëse qëllimi i përpunimit nuk mund të jetë i arsyeshëm që të arrihet në ndonjë mënyrë tjetër. Kjo imponon kufizim të periudhës për ruajtjen e të dhënave personale në periudhë më të shkurtë të mundshme.

- **Ø Saktësi**

Kontrolluesit duhet të sigurohen se të dhënat personale janë të sakta dhe kur ajo është e nevojshme të azhurnohen, me marrjen e të gjitha hapave të arsyeshëm/masa për shlyerje ose korrigjim të të dhënave personale të pasakta pa prolongim të panevojshëm dhe në pajtim me qëllimin e për të cilin përpunohen. Konkretisht, kontrolluesi duhet saktë t'i regjistrojë informacionet të cilat i grumbullojnë ose marrin, së bashku me burimin e informacioneve të tilla.

- **Ø Kufizimi i afatit për ruajtje**

Të dhënat personale duhet të ruhen në formë e cila lejon identifikimin e subjektit të të dhënave personale vetëm në periudhë që është e nevojshme për qëllime të cilat përpunohen. Që të sigurohet se të dhënat personale nuk ruhen më gjatë se sa është e nevojshme kontrolluesit duhet të caktojnë afat kohor për shlyerjen e të dhënave personale ose për revizion periodik.

- **Ø Integritet dhe besueshmëri**

Të dhënat personale duhet të përpunohen në mënyrë e cila garanton siguri adekuate dhe besueshmëri të tyre, duke përfshirë edhe mbrojtje nga qasja e paautorizuar ose e paligjshme ose shfrytëzimin e të dhënave personale dhe pajisjen që shfrytëzohet për përpunim, si dhe nga humbja e rastësishme, shkatërrimi ose dëmtimi, përmes zbatimit të masave adekuate teknike dhe organizative.

- **Ø Llogaridhënia**

Në fund, kontrolluesit janë përgjegjës për dhe duhet të demonstrojnë harmonizim me të gjitha parimete lartpërmendura për mbrojtjen e të dhënave personale. Përkatësisht, kontrolluesi duhet t'i ndërmarrë përgjegjësitë për përpunimin e të dhënave personale dhe harmonizim me LMDHP, dhe të jenë në mundësi ta dëshmojnë atë, duke përfshirë edhe para AMDHP, me dorëzimin e evidencës adekuate dhe zbatimin e masave.

Më shumë informacione për parimin e mbrojtjes së të dhënave personale mund të lexoni në Udhëzuesin për parimin për mbrojtjen e të dhënave personale të arritshme në linkun si vijon link

2.2.2. BAZA LIGJORE PËR PËRPUNIMIN E TË DHËNAVE PERSONALE

Kontrolluesit/përpunuesit duhet të kenë bazë ligjore për përpunim të të dhënave personale.

Sipas LMDHP, ekzistojnë gjashtë baza ligjore të përpunimit. Kontrolluesit janë të obliguar të sigurojnë përpunim ligjor të të dhënave personale. Bazat e mundshme juridike për përpunim ligjor janë:

- **Ø Pëlqimi i subjektit të të dhënave personale**

Subjekti i të dhënave personale i jep pëlqim kontrolluesit për përpunim të të dhënave personale të tij/saj për një ose më shumë qëllime të përpunimit. Pëlqimi duhet të jetë dhënë lirshëm, qartë dhe duhet të mund të tërhiqet lehtë , prandaj kontrolluesi duhet të jetë i vëmendshëm kur shfrytëzon pëlqim si bazë juridike për përpunimin e të dhënave personale. Në këtë drejtim, GDPR u dha fund praktikave me fusha të selektuara automatikisht për pëlqim.

- **ØRealizimi i marrëveshjes ku njëra palë është subjekt i të dhënave personale**

Kjo bazë juridike nënkupton situatë në të cilën aktiviteti për përpunimin e të dhënave personale është i nevojshëm për lidhjen ose realizimin e marrëveshjes. Nëse aktiviteti nuk lidhet me kushtet e marrëveshjeve, atëherë përpunimi i të dhënave personale duhet të jetë i përfshirë me bazë ligjore tjetër.

- **ØDetyrimi ligjor i kontrolluesit**

Këtu hyjnë situata ku aktiviteti për përpunim të të dhënave personale është i nevojshëm për plotësimin e ndonjë obligimi të përcaktuar me ligjin të cilën e zbaton kontrolluesi, për shembull, për marrëdhënie pune, për mbrojtjen e konsumatorëve etj.

- **ØMbrojtja e jetës ose interesit esencial të subjektit të të dhënave personale**

Kjo bazë juridike shfrytëzohet në situata të rralla kur aktivitet për përpunim të të dhënave personale mund të jenë të nevojshme për shpëtimin e jetës të dikujt, që më shpesh është lidhur me nevojën për ndihmë urgjente mjekësore.

- **ØKryerja e punëve me interes publik ose autorizim publik**

Aktivitet për përpunimin e të dhënave personale të cilin e kryejnë organet e administratës shtetërore ose organizata të cilat kryejnë autorizime publike në emër të organeve të administratës shtetërore.

- **ØInteresi legjitim**

Kjo nënkupton aktivitet për përpunim të të dhënave personale të cilin subjekti i të dhënave personale zakonisht e pret nga organizata e cila i lëshon të dhënat e tyre personale, për shembull aktivitete marketingu ose pengim të mashtrimit. Kur organizata shfrytëzon interes legjitim si bazë juridike për përpunim, ajo duhet të zbatojë test për balancim, respektivisht të konstatojë nëse aktiviteti për përpunim është i domosdoshëm që organizata të funksionojë ta kryejë veprimtarinë e saj ose nëse aktiviteti për përpunim ka përparësi para të drejtave dhe lirive të subjektit të të dhënave personale. Nëse përgjigjja e ndonjë nga këto pyetje është negative, atëherë organizata nuk mund të shfrytëzojë interesin legjitim si bazë juridike për përpunim.

Më shumë informacione për ligjshmërinë e përpunimit të të dhënave personale mund të lexoni në Udhëzuesin për ligjshmëri të përpunimit të të dhënave personale të arritshëm në linkun si vijon link.

Ky projekt financohet nga Bashkimi Evropian

2.2.3. njoftimi për përpunim (të të dhënave personale) me rrezik të lartë

Kur gjatë shfrytëzimit të teknologjive për ndonjë lloj të përpunimit, duke marrë parasysh natyrën, vëllimin, kontekstin dhe qëllimet e përpunimit të të dhënave personale, ekziston mundësia që e njëjta të shkaktojë rrezik për të drejtat dhe liritë e personave fizikë, në funksion të nenit 9 nga LMDHP, kontrolluesi e njofton Agjencinë për Mbrojtjen e të Dhënave Personale përmes evidencës elektronike të përmbledhjes së të dhënave personale përpunimi i të cilave është me rrezik të lartë e arritshme në linkun në vijim.

2.2.4. Detyrimi i ri NJOFTIM PËR CENIMIN E SIGURISË sË TË DHËNAVE PERSONALE

GDPR dhe Ligji i ri për mbrojtjen e të dhënave personale në Maqedoninë e Veriut inkorporojnë detyrim të ri për kontrolluesit në rast të cenimit të sigurisë së të dhënave personale[1] gjë që nënkupton njoftim të organit mbikëqyrës (AMDHP) dhe të subjekteve të prekura të të dhënave personale
Përkatësisht, kontrolluesit janë të obliguar ta informojnë Agjencinë për cenimin e sigurisë së të dhënave personale përveç nëse nuk ekziston mundësia që cenimi do të rezultojë me rrezik për të drejtat dhe liritë e subjektit të të dhënave personale. Nga këtu, për çdo cenim të sigurisë së të dhënave personale kontrolluesi duhet të vlerësojë nëse ekziston detyrim për njoftim të Agjencisë.

Shembull: Kontrolluesi duhet ta njoftojë Agjencinë për humbjen e të dhënave personale të shfrytëzuesve sepse ngjarja e tillë mund të çojë deri te vjedhja e identitetit, por nuk duhet ta njoftojë Agjencinë në rast të humbjes së të dhënave të cilat kanë të bëjnë me listën e numrave të telefonit të të punësuarve, sepse cenimi i tillë nuk ndikon në të drejtat dhe liritë e subjekteve të të dhënave personale.

[1] „Cenimi i sigurisë të të dhënave personale” është çdo cenim i sigurisë, që sjell deri tek shkatërrimi i rastësishëm ose shkatërrim i paligjshëm, humbje, ndryshim, zbulim i paautorizuar ose qasje deri tek të dhënat që barten, ruhen ose në mënyrë tjetër përpunohen.

Në rast kur ekziston mundësia që cenimi i sigurisë së të dhënave personale të rezultojë me rrezik të lartë për të drejtat dhe liritë e subjektit të të dhënave personale[1], kontrolluesi drejtpërdrejtë duhett'i njoftojë subjektet e interesuara.
Kontrolluesit nuk kanë detyrim për njoftim të subjekteve të të dhënave personale për cenimin e sigurisë së të dhënave personale në rastet si vijojnë:

- Ø Kur kontrolluesi ka zbatuar masa adekuate teknike dhe organizative, duke përfshirë edhe masa në raport të të dhënave personale të prekura nga cenimi;
- Ø kur kontrolluesi ka ndërmarrë masa plotësuese që garantojnë se tashmë nuk ekziston mundësi për paraqitje të rrezikut të lartë për të drejtat dhe liritë e subjekteve të të dhënave personale;
- Ø kur dorëzimi i njoftimit të tillë paraqet përpjekje tejet të madhe, me ç'rast kontrolluesi mund të bëjë njoftim publik ose ndonjë masë të ngjashme efektive për njoftim të subjektit.
-

Nëse kontrolluesi nuk e njofton subjektin e të dhënave personale dhe Agjencinë për cenimin konkret të sigurisë së të dhënave personale që paraqet rrezik të lartë për të drejtat dhe liritë e subjektit, Agjencia mund të kërkojë nga kontrolluesi:

- Ø t'i njoftojë subjektet për cenimin konkret; ose
- Ø të dëshmojë se plotëson një nga kushtet për të cilat nuk ekziston detyrim për njoftim.

Njoftimin që kontrolluesit e dorëzojnë te Agjencia duhet t'i përmbajë informacionet si vijojnë:

- Ø përshkrim të natyrës së cenimit dhe, nëse është e mundshme, kategoritë dhe numrin e përafërt të subjekteve të prekura të të dhënave personale dhe numrin e përafërt të të dhënave personale të evidentuara të prekura.

[1] Për rrezik të lartë për të drejtat dhe liritë e subjektit të të dhënave personale konsiderohet dëm fizik material ose jomaterial për subjektet, siç është humbja e kontrollit mbi të dhënat e tyre personale, kufizimi i të drejtave, diskrimin, vjedhje e identitetit, mashtrim me identitet të rrejshëm, humbje financiare, cenimi i besueshmërisë të të dhënave personale ose çfarëdo pasoje tjetër negative ekonomike ose sociale mbi personin e prekur.

- Ø emrin/mbiemrin dhe detajet kontaktuese të oficerit për mbrojtjen e të dhënave personale ose të personit tjetër për kontakt nga i cili mund të merren më shumë informata;
- Øpërshkrimin e pasojave të mundshme nga cenimi i sigurisë së të dhënave personale;
- Ø përshkrimin e masave të propozuara ose të marra nga ana e kontrolluesit për ballafaqim me cenimin ose për uljen e efekteve negative.

Përmbajtja e njoftimit për subjektet e të dhënave personale duhet të jetë e njëjta, por natyra e cenimit duhet të përshkruhet në gjuhë më të thjeshtë.

Gjithashtu, njoftimi duhet të parashtrohet menjëherë por jo më vonë se 72 orë pasi që kontrolluesi ka kuptuar për cenimin e sigurisë së të dhënave personale. Nëse kontrolluesi nuk parashtron njoftim të tillë në afat prej 72 orëve, atëherë së bashku me njoftimin që dorëzohet më vonë duhet të arsyetohen edhe shkaqet e vonesës.

Detyrimi për dokumentim

Kontrolluesit janë të detyruar t’i dokumentojnë të gjitha cenimet e sigurisë së të dhënave personale, duke përfshirë edhe faktet lidhur me cenimin, pasojat dhe aktivitetet që janë ndërmarrë për ballafaqim me të njëjtën. Dokumentacioni i tillë i mundëson Agjencisë ta kontrollojë harmonizimin me nenin 37 nga LMDHP.

2.2.5. Evidenca e aktiviteteve për përpunim

Sipas nenit34 nga LMDHP, kontrolluesit dhe, kur është përkatëse, përfaqësuesit e kontrolluesit mbajnë evidencë për aktivitetet për përpunimin e të dhënave personale për të cilat janë përgjegjëse.

Evidenca e tillë duhet t’i përmbajë informacionet si vijojnë:
(titullin, respektivisht emrin/mbiemrin dhe kontakt detajet e kontrolluesit dhe, kur është e përshtatshme, të të gjithë kontrolluesve të përbashkët, personave të autorizuar të kontrolluesit dhe oficerit për mbrojtjen e të dhënave personale;
(b) qëllimet e përpunimit;

(v) përshkrimin e kategorive të subjektit të të dhënave personale dhe kategorive të të dhënave personale.
(g) kategoritë e shfrytëzuesve të cilëve u janë zbuluar ose do tu zbulohen të dhënat personale, duke përfshirë edhe shfrytëzues në vende të treta ose organizata ndërkombëtare;
(d) kur është e përshtatshme, bartja e të dhënave personale në vende të treta ose organizata ndërkombëtare, duke përfshirë edhe identifikim të vendeve të treta ose organizata ndërkombëtare, derisa në rast të bartjes të të dhënave personale sipas nenit53, paragrafi (1), alineja 2) nga LMDHP, dokumentacioni për zbatimin e masave mbrojtëse adekuate;
(gj) kur është e përshtatshme, afati i paraparë për shlyerje të kategorive të ndryshme të të dhënave personale;
(e) kur është e përshtatshme, përshkrimi i përgjithshëm i masave organizative dhe teknike sipas nenit 36, paragrafit (1) të LMDHP.

2.3. Ndjekja e harmonizimit me lmdhp

Oficerët për mbrojtjen e të dhënave personale e ndjekin harmonizimin me LMDHP, dispozitat tjera të Republikës së Maqedonisë së Veriut dhe politikat e kontrolluesit/përpunuesit të cilat kanë të bëjnë në mbrojtjen e të dhënave personale, duke përfshirë edhe shpërndarjen e përgjegjësive, ngritjen e vetëdijes dhe trajnimit të të punësuarve të cilët kanë marrë pjesë në operacionet për përpunim, si dhe zbatimin e revizioneve dhe mbrojtjen e të dhënave personale (neni 43, paragrafi (1), pika (b) nga LMDHP).

Konkretisht, oficeri ndihmon në sigurimin e harmonizimit të brendshëm me këto dispozita. Ai/ajo grumbullon informacione për identifikim të operacioneve për përpunim të të dhënave personale, analizë dhe vërtetim të harmonizimit, dhe jep informacione, këshilla dhe rekomandime të kontrolluesit.

Oficeri nuk është personalisht përgjegjës në rast të mosharmonizimit me dispozitat për mbrojtjen e të dhënave personale. Harmonizimi me këto dispozita është përgjegjësi e kontrolluesit.

GDPR/LMDHP qartë përcaktojnë se kontrolluesi siguron harmonizim me dispozitat nga rregullativa/ligjidhe demonstron se përpunimi i të dhënave personale kryhet në pajtim me të njëjtat, derisa oficeri për mbrojtjen e të dhënave personale është figura kryesore përmes të cilës kontrolluesi e plotëson këtë detyrim.

Harmonizimi dhe ndjekja e harmonizimit me dispozitat për mbrojtjen e të dhënave personale nënkupton: respektimin e parimit për mbrojtjen e të dhënave personale gjatë përpunimit të të dhënave personale nga ana e kontrolluesit; përgatitjen e dokumentacionit dhe zbatimin e masave teknike dhe organizative, përpunimin e politikës/deklaratës për privatësi dhe azhurnim të rregullt të të njëjtës; informimin për grumbullimin e të dhënave personale dhe respektimin e rregullave për video mbikëqyrje. Zgjidhja e re ligjore vendos edhe detyrim për kontrolluesit për njoftim për cenimin e sigurisë së të dhënave personale.

2.4. ngritja e vetëdijes për mbrojtjen e të dhënave personale

Ngritja e vetëdijes mes të punësuarve te kontrolluesi për të drejtën e mbrojtjes së të dhënave personale është një nga detyrat kryesore të punës së oficerit për mbrojtjen e të dhënave personale e cila e afirmon këtë të drejtë të personave fizikë dhe e edukon kontrolluesin për obligimet të cilat dalin nga dispozitat për mbrojtjen e të dhënave personale.

Oficeri për mbrojtjen e të dhënave personale duhet të shfrytëzojë sa është e mundshme më shumë aktivitete për vetëdije në kuadër të kontrolluesit, veçanërisht mes të punësuarve të cilët janë të përfshirë drejtpërdrejt në operacionet për përpunim të të dhënave personale.

2.5. trajnimi i të punësuarve

LMDHP përcakton detyrim për oficerët për mbrojtjen e të dhënave personale të kryejnë trajnim të të punësuarve në raport të mbrojtjes së të dhënave personale.

Në pajtim me nenin 69 nga LMDHP, Agjencia përgatit dhe zbaton trajnim për të punësuarit te kontrolluesit dhe përpunuesit, si dhe për oficerët për mbrojtjen e të dhënave personale. Pas trajnimit të zbatuar, AMDHP lëshon certifikatë për trajnim të mbaruar dhe mban evidencë për këtë. Qëllimi i këtyre trajnimeve është të punësuarit te kontrolluesit dhe përpunuesit të fitojnë njohuri në fushën e mbrojtjes të të dhënave personale, kurse oficeri të fitojë njohuri dhe aftësi për dispozitat dhe praktikat në fushën e mbrojtjes së të dhënave personale dhe të zhvillojnë aftësi për kryerjen e detyrave të cilat janë përcaktuar në nenin 43 nga LMDHP.

2.6. dhënia e këshillave dhe rekomandimeve për kontrolluesit/përpunuesit

Detyrimet e oficerit për mbrojtjen e të dhënave personale përfshijnë edhe dhënien e këshillave të kontrolluesit për plotësimin e detyrimeve të cilat dalin nga dispozitat për mbrojtjen e të dhënave personale dhe rekomandimet për përmirësim praktik të mbrojtjes të të dhënave personale.

Këshillat mund të jepen gojarisht ose me shkrim. Nëse ndonjë këshillë e dhënë për rast konkret mund të zbatohet në raste tjera të ngjashme, rekomandohet ajo të publikohet në ueb faqen e kontrolluesit. Në rast kur oficeri ka dilema për atë se çfarë këshille t'i japë kontrolluesit, rekomandohet që ai/ajo të konsultohet me organin mbikëqyrës (AMDHP).

Oficeri jep i rekomandime kontrolluesit/ përpunuesit për përmirësim praktik të mbrojtjes së të dhënave personale. Këto rekomandime mund të jepen me vetiniciativë ose me kërkesë nga kontrolluesi/përpunuesi.

2.7. REVIZONEt/ KONTROLLEt/ SHQYRTIMEt

Oficeri për mbrojtjen e të dhënave personale duhet të jetë i autorizuar, vetë ose me ndihmë nga të tjerët, të kryejë revizion/kontroll/ shqyrtim të harmonizimit të kontrolluesit me dispozitat për mbrojtjen e të dhënave personale. Për këtë qëllim, kontrolluesi duhet t'i sigurojë oficerit qasje te të gjithë informacionet dhe dokumentet relevante .

Procedura dhe mënyra për kryerjen e revizioneve/kontrolleve/ shqyrtimeve ngaoficeri për mbrojtjen e të dhënave personale duhet të jenë të rregulluara me akt intern të kontrolluesit.

2.8. vlerësimi i ndikimit mbi mbrojtjen e të dhënave personale

Shfrytëzimi i mjeteve për vlerësim të ndikimit të operacioneve të planifikuara për përpunim mbi mbrojtjen e të dhënave personale (VNMDHP)[1] është mënyra më efektive për sigurimin e pëlqimit me dispozitat për mbrojtjen e të dhënave personale dhe për plotësimin e pritjeve të subjektit të të dhënave personale në raport të privatësisë.

[1] Rregullore për procesin e vlerësimit të ndikimit mbi mbrojtjen e të dhënave personale e arritshme në linkun si vijon

Përkatësisht, neni 39 nga LMDHP përcakton se në rastet kur shfrytëzohen teknologji të reja për ndonjë lloj përpunimi, dhe kur sipas natyrës, vëllimit, kontekstit dhe qëllimeve të përpunimit, ekziston mundësia që përpunimi i tillë do të rezultojë me rrezik të lartë për të drejtat dhe liritë e personit fizik, para se të fillojë me përpunim, kontrolluesi duhet të bëjë vlerësim të ndikimit mbi mbrojtjen e të dhënave personale. Një vlerësim mund të paraqesë seri të operacioneve të ngjashme për përpunim të cilat paraqesin rrezik të lartë të ngjashëm.

Edhe pse zbatimi i vlerësimit të tillë është detyrë e kontrolluesit, oficeri për mbrojtjen e të dhënave personale ka rol të rëndësishëm përmes dhënies së këshillave konkrete dhe ndjekjes nëse kontrolluesi i respekton këshillat e dhëna dhe të pranuara. Nëse kontrolluesi nuk e pranon këshillën e oficerit, kjo duhet të dokumentohet më mënyrë adekuate, së bashku me arsyetimin e shkaqeve për mospranimin e tillë.

Ky mjet i mundëson kontrolluesve t’i identifikojnë dhe zgjedhin problemet që në fazë të hershme të zhvillimit të sistemeve të reja dhe prodhime të reja, dhe t’i ulë shpenzimet e panevojshme dhe dëmin potencial material për reputacionin e tyre si pasoja të mundshme negative.

Ky mjet veç më është vendosur dhe shfrytëzohet nga ana e disa kontrolluesve në sektorin privat, veçanërisht ato të cilët punojnë në sektorin bankar dhe në fushën e komunikimeve elektronike.

Në pajtim me nenin 39, paragrafi (3) nga LMDHP, vlerësimi i ndikimit mbi mbrojtjen e të dhënave personale është i detyrueshëm në rastet si vijojnë:
((a) vlerësim sistemor gjithëpërfshirës i aspekteve personale të cilat janë lidhur me personat fizikë , i cili bazohet në përpunimin automatik, duke përfshirë edhe profilim, kurse i cili shërben si bazë për miratimin e vendimeve që prodhojnë veprim juridik në lidhje me personin fizik ose ndikojnë në mënyrë të konsiderueshme mbi personin fizik;
(b) përpunim voluminoz i kategorive të posaçme të të dhënave personale në pajtim me nenin 13 nga LMDHP ose të të dhënave personale lidhur me dënime penale ose vepra penale në pajtim me nenin 14 nga LMDHP;ose
(c) mbikëqyrje sistemore e hapësirave publike me përmasa të mëdha.

Me këtë rast, vlerësimi duhet t’i përmbajë informacionet si vijojnë:

përshkrim sistematik operacione të parapara për përpunim edhe qëllimet e përpunimit, duke përfshirë edhe interes legjitim të kontrolluesit, kur ajo është e zbatueshme;
b) vlerësimi i domosdoshmërisë dhe proporcionalitetit të operacioneve për përpunim në raport të qëllimeve;
v) vlerësim i rreziqeve për të drejtat dhe liritë e subjektit të të dhënave personale nga neni 39, paragrafi (1) nga LMDHP; dhe
g) masa të parapara për zgjidhjen e rreziqeve, duke përfshirë edhe masat mbrojtëse, masat dhe mekanizmat për siguri të të dhënave personale dhe për demonstrim të harmonizimit me LMDHP, duke marrë parasysh të drejtat dhe interesat legjitime të subjektit të të dhënave personale dhe personat tjerë të prekur.

Në pajtim me nenin 39, paragrafi (4) dhe paragrafi (5) nga LMDHP, Agjencia për Mbrojtjen e të Dhënave personale së bashku me rregulloren ka miratuar dhe publikuar dy lista të llojeve të operacioneve për përpunimin e të dhënave personale të cilat imponojnë/nuk imponojnë vlerësim të detyrueshëm të ndikimit mbi mbrojtjen e të dhënave personale.[1][2]

Në pajtim me Udhëzimet për oficerët për mbrojtjen e të dhënave personale të përpunuara nga grupi punues 29 (GP29), zbatimi i vlerësimit të ndikimit mbi mbrojtjen e të dhënave personale (neni 35, paragrafi (1) nga GDPR) është detyrë e kontrolluesve, por jo e oficerëve. Megjithatë, oficerët mund të kenë rol shumë të rëndësishëm dhe të favorshëm përmes këshillimit të kontrolluesve për plotësimin e këtij detyrimi.

Kush është i obliguar të zbatojë vlerësim të ndikimit?
LMDHP përcakton se obligimi për zbatimin e vlerësimit të ndikimit mbi mbrojtjen e të dhënave personale bie te kontrolluesit, dhe kjo duhet të bëhet në konsultim me oficerin për mbrojtjen e të dhënave personale dhe me përpunuesit (neni 39, paragrafi (1) dhe paragrafi (2)). Vlerësimin e ndikimit mund ta bëjë çdo person tjetër, në dhe jashtë organizatës, por përgjegjësia përfundimtare për plotësimin e këtij detyrimi mbetet te kontrolluesi.[1]

[2] Lista e llojeve të operacioneve për përpunim për të cilat kërkohet ndikimi mbi mbrojtjen e të dhënave personale është e arritshme në likun si vijon.
[1] Rregullore për procesin e vlerësimit të ndikimit mbi mbrojtjen e të dhënave personale e arritshme në linkun si vijon.

Kur është caktuar oficer për mbrojtjen e të dhënave personale, kontrolluesi është i detyruar të kërkojë këshillë gjatë zbatimit të vlerësimit të ndikimit (neni 39, paragrafi (2) nga LMDHP), me ç’rast këshilla, si dhe vendimi i kontrolluesit nëse e pranon ose e refuzon, duhet të jetë e dokumentuar në VNMDHP. Nga ana tjetër, oficeri e ndjek zbatimin e vlerësimit të ndikimit (neni 43, paragrafi (1), alineja (v)) nga LMDHP) Nëse kontrolluesi ka angazhuar përpunues i cili është i detyruar për përpunim të plotë ose të pjesshëm të të dhënave personale, përpunuesi i ndihmon kontrolluesit në zbatimin e vlerësimit të ndikimit dhe i siguron të gjitha informacionet e nevojshme (neni 32, paragrafi (3), alineja (gj) nga LMDHP).

GP29 rekomandon kontrolluesit të kërkojnë këshillë nga oficeri për mbrojtjen e të dhënave personale për çështjet si vijojnë:

- · nëse duhet të zbatohet vlerësim i ndikimit mbi mbrojtjen e të dhënave personale
- · cila metodologji duhet të zbatohet për zbatimin e vlerësimit të ndikimit mbi mbrojtjen e të dhënave personale;
- · nëse zbatimi i vlerësimit të ndikimit të bëhet në vetë organizatën ose të angazhohet person i jashtëm;
- · çfarë masa mbrojtëse, duke përfshirë edhe masa teknike dhe organizative të zbatohen për zbutjen e rreziqeve të mundshme për të drejtat dhe interesat e subjektit të të dhënave personale;
- · nëse vlerësimi i ndikimit është zbatuar në mënyrë konkrete dhe nëse konkluzionet nga e njëjta në lidhje me vazhdimin e përpunimit dhe masat mbrojtëse që do të zbatohen janë në pajtim me LMDHP.

Nëse kontrolluesi nuk pajtohet me këshillën e dhënë nga oficeri për mbrojtjen e të dhënave personale, dokumentacioni lidhur me vlerësimin e ndikimit mbi mbrojtjen e të dhënave personale duhet të përfshijë arsyetim të shkaqeve pse këshilla e oficerit nuk është marrë parasysh.

Udhëzime më të detajuara janë dhënë në Udhëzimet për oficerët për mbrojtjen e të dhënave personale të lëshuara nga GP29.

2.8. bashkëpunimi me amdhp dhe veprimi si pikë kontakti

Në pajtim me nenin 43 nga LMDHP, oficeri për mbrojtjen e të dhënave personale vepron si pikë kontakti për Agjencinë në raport me çështjet lidhur me përpunimin, duke përfshirë edhe konsultime paraprake në pajtim me nenin 40 nga LMDHP, si dhe këshillim për çështje tjera, kur kjo është e përshtatshme.

Oficerët për mbrojtjen e të dhënave personale nga sektori privat dhe publik veç më kanë vendosur bashkëpunim me AMDHP i cili përfshin përkrahje nga Agjencia për çështje lidhur me kryerjen e funksionit të tyre, ndarja e informacioneve dhe komunikim tjetër. Bashkëpunimi i tillë i mundëson AMDHP me rregullshmëri ta ndjekë harmonizimin me dispozitat për mbrojtjen e të dhënave personale. Përveç kësaj, oficerët marrin pjesë edhe në trajnimet që i organizon AMDHP të cilat nuk konsiderohen vetëm si mjet për thellimin dhe mbindërtimin e njohurive të tyre profesionale, por edhe si mënyrë për forcimin e bashkëpunimit me Agjencinë dhe mes oficerëve.

Forcimi i bashkëpunimit mes AMDHP dhe kontrolluesve është me rëndësi esenciale për vendosjen e standardeve më të larta në raport të respektimit të të drejtës të mbrojtjes së të dhënave personale, kurse oficerët kanë rol qendror në forcimin e bashkëpunimit të tillë.

Oficerët për mbrojtjen të dhënave personale veprojnë si pikë kontakti e cila e lehtëson komunikimin mes AMDHP dhe kontrolluesit.

Roli i tillë i “lehtësuesve” është dhënë edhe në hyrjen nga Udhëzimet e GP29. Përkatësisht përmes veprimit si pikë kontakti, oficerët e lehtësojnë qasjen e organit mbikëqyrës te dokumenti dhe informacioni për plotësimin e detyrave të theksuara në nenin 65 nga LMDHP, si dhe për kryerjen e autorizimeve korrigjuese dhe hulumtuese, dhënien e lejes dhe mendimeve sipas nenit 66 nga LMDHP.

Ashtu siç ishte përmendur, oficerët për mbrojtjen e të dhënave personale janë të obliguar në fshehtësi dhe besueshmëri gjatë kryerjes të detyrave të tilla, në pajtim me ligjin (neni 42, paragrafi (5) nga LMDHP). Megjithatë, detyrimi për fshehtësi dhe besueshmëri nuk i pengon oficerët ta kontaktojnë dhe të kërkojnë këshillë nga organi mbikëqyrës. Përkatësisht, neni 43 paragrafi (1) pika (g) nga LMDHP, përcakton se oficeri për mbrojtjen e të dhënave personale mund ta konsultojë organin mbikëqyrës për të gjitha çështjet, kur kjo është përkatëse.

2.9. masat organizative dhe teknike për siguri të të dhënave personale

Për qëllimet e plotësimit të detyrimeve nga LMDHP dhe Rregullores për Siguri të Përpunimit të të Dhënave personale, kontrolluesit miratojnë dokumentacion dhe zbatojnë masa teknike dhe organizative për siguri dhe besueshmëri të përpunimit të të dhënave personale nga qasja e rastësishme ose e paautorizuar, ndryshimi, zbulimi, humbja ose asgjësimi i të dhënave.

Një nga detyrat primare të oficerit për mbrojtjen e të dhënave personale është ta ndjekë harmonizimin e kontrolluesit me këtë dokumentacion.

Sipas nenit 28, paragrafi (1) nga LMDHP, duke marrë parasysh natyrën, vëllimin, kontekstin dhe qëllimet e përpunimit, si dhe rreziqet me shkallë të ndryshme të besueshmërisë dhe serioziteti për të drejtat dhe liritë e personave fizikë, kontrolluesit zbatojnë masa adekuate teknike dhe organizative që të sigurohen dhe të jenë në mundësi të dëshmojnë se përpunimi kryhet në pajtim me ligjin. Sipas nevojës, masat teknike dhe organizative janë lëndë e revizionit dhe azhurnimit.

Sipas nenit 36, paragrafi (1) nga LMDHP, duke marrë parasysh arritjet më të reja teknologjike, shpenzimet për zbatimin, natyrën, vëllimin, kontekstin dhe qëllimet e përpunimit, si dhe rreziqet deri në shkallë të ndryshme të besueshmërisë dhe seriozitetin për të drejtat dhe liritë e personave fizikë, kontrolluesit dhe përpunuesit zbatojnë masa adekuate teknike dhe organizative që të sigurojnë nivel të sigurisë adekuat me rrezikun, duke përfshirë edhe:
((a) psuedonimizim dhe kriptim të të dhënave personale;
(b) aftësinë për sigurimin e besueshmërisë së vazhdueshme, integritetit, qasjes dhe rezistencës së sistemit dhe shërbimeve për përpunim;

(v) aftësinë për rivendosje në kohë të qasjes te të dhënat personale dhe qasjen deri tek ato në rast të incidenti fizik ose teknik;
(g) procesin e testimit të rregullt, vlerësim dhe evaluim të efektivitetit të masave teknike dhe organizative që të garantohet siguri e përpunimit.

SI TË KONSTATOHET CILAT MASA TEKNIKE DHE ORGANIZATIVE JANË PËRKATËSE PËR KONTROLLUESIN?

Hapi 1: Përshkruani aktivitetet për përpunimin e të dhënave personale
Çfarë lloj i të dhënave personale përpunohen? Cili, kur dhe për çfarë qëllimi? Çfarë sisteme shfrytëzohen për përpunim të të dhënave personale?

Hapi 2: Kontrolloni bazat juridike për përpunim të të dhënave personale
Nëse të dhënat personale mblidhen dhe përpunohen në mënyrë ligjore? Nëse të dhënat personale evidentohen për qëllim konkret dhe nëse ndiqen udhëzimet për përpunimin e të dhënave personale?

Hapi 3: Përcaktoni cilat procese afariste imponojnë siguri më të madhe
Cilat shërbime, sisteme, hapësira dhe të dhëna duhet të jenë të mbrojtura? Si janë të lidhura ato mes veti?

ЧHapi 4: Analizoni rreziqet potenciale
Identifikimi i rreziqeve: Nëse siguria e të dhënave personale është e nënshtruar në rreziqe siç janë katastrofat natyrore, përgjegjësi të definuara në mënyrë të paqartë në kuadër të organizatës, ose potencialisht probleme teknike?

Vlerësimi i pasojave të mundshme: Sa është serioziteti i pasojave në rast të incidentit? Nëse skenari për rast më të keq ndikon mbi të dhënat të cilat duhet në veçanti të jenë të mbrojtura, si për shembull, të dhëna për shëndetin ose detaje nga dosja e personit të punësuar?
Vlerësimi i besueshmërisë: Sa është besueshmëria të ndodhë ndonjë incident? Çfarë përvojë ka organizata e cila mund ta lehtësojë vlerësimin e seriozitetit të dëmit nga ngjarja e tillë? Çfarë informacione duhet të merren parasysh që të mund të konstatohet dëmi i mundshëm?

Përcaktimi i shkallës së rrezikut: Cilat rreziqe nënkuptojnë shkallë të lartë të seriozitetit dhe shkallë të lartë të mundësisë? Cilat rreziqe do kishin shkaktuar dëm më të vogël dhe për cilat rreziqe ekziston mundësi më e vogël të paraqiten?

Hapi 5: Zgjidhini masat adekuate teknike dhe organizative
Cilat rreziqe duhet të zgjidhen për shkak të shkallës së lartë të seriozitetit dhe mundësisë? Duke marrë parasysh arritjet më të reja teknologjike, cilat masat konkrete duhet të shqyrtohen për minimizim të këtyre rreziqeve? Cilat masa mund të zbatohen në vëllim të arsyeshëm (përfaqësojnë shpenzim racional, për shembull)?

Hapi 6: vlerësimi i rrezikut të mbetur
Cilat rreziqe mund të jenë tërësisht të eliminuara me zbatimin e masave teknike dhe organizative? Sa është shkalla e seriozitetit dhe mundësia e rreziqeve tjera?

Hapi 7: Konsolidoni masat
A duhet të kombinohen masat e ndryshme apo masat individuale janë të mjaftueshme? A janë masat e përshtatshme me rrethanat e posaçme në organizatën tuaj?

Hapi 8: Zbatoni masat e zgjedhura
Cilat masa duhet së pari t'i zbatoni?. Kush do të marrë përgjegjësi për zbatimin e tyre?. Nëse zbatimi i masave ka sjellë deri te rezultati i dëshiruar?

2.9. qasje që bazohet në rrezik

Në pajtim me dispozitat, gjatë kryerjes së detyrave, oficerët për mbrojtjen e të dhënave personale duhet të marrin parasysh rreziqet lidhur me operacionet për përpunim, si dhe natyrën, vëllimin dhe qëllimet e përpunimit të të dhënave personale. Kjo do të thotë se oficeri vë prioritet dhe fokusohet në çështjet të cilat paraqesin rrezik të lartë pas mbrojtjes së të dhënave personale. Sipas kësaj qasje pragmatike, oficerët përcaktojnë se cilat fusha janë lëndë dhe cilat duhet të jenë lëndë e revizionit të brendshëm ose të jashtëm revizion/kontroll/shqyrtim, çfarë trajnimi duhet të organizohet për të punësuarit dhe cilat operacione për përpunim të punësuarit duhet t’i kushtojnë vëmendje më të madhe.

Në pajtim me Rregulloren për Siguri të Përpunimit të të Dhënave Personale[1], gjatë identifikimit dhe vlerësimin e rreziqeve (menaxhim me rreziqe), kontrolluesit i marrin parasysh rreziqet të cilat janë lidhur me përpunimin e të dhënave personale, veçanërisht nga asgjësimi i rastësishëm ose i paligjshëm, humbja, ndryshimi, zbulimi i paautorizuar ose qasje e paautorizuar te të dhënat të cilat janë bartur, ruhen ose në mënyrë tjetër përpunohen.

Kontrolluesit janë përgjegjës për harmonizimin e nivelit të masave për siguri të përpunimit të cilat i zbatojnë në pajtim me nenin 8 të Rregullores, me ç’rast duhet të sigurohet nivel adekuat i sigurisë së të dhënave personale, duke përfshirë dhe mbrojtjen nga përpunimi i paautorizuar ose jo ligjor i të dhënave personale, si dhe mbrojtja nga humbja e tyre e rastësishme, asgjësimi ose dëmtimi.

Megjithatë, gjatë kryerjes së detyrave të tyre dhe në bazë të natyrës, vëllimit, kontekstit dhe qëllimeve të përpunimit, oficerët për mbrojtjen e të dhënave personale duhet të marrin parasysh rreziqet lidhur me operacionet për përpunimin e të dhënave personale. Plotësimi i këtyre kushteve imponon përcaktim të rreziqeve relevante. Kjo duhet të bëhet përmes përgatitjes së inventarit të operacioneve për përpunimin e të dhënave personale dhe krijimin e regjistrit të operacioneve të tilla, si dhe zbatimit të kontrollit të rregullt të operacioneve të tilla.

Më pas, elementet e rrezikut dhe raportet etyre mund të jenë të ilustruara në diagram si ai i dhënë më poshtë:

Vlerësim adekuat i rreziqeve zbatohen në katër hapa:

1.1. Definimi i operacionit për përpunim dhe konteksti i tyre.
2.2. Kuptimi dhe evaulimi i ndikimit.
3.3. Definimi i kërcënimeve të mundshme dhe evaluimi i mundësisë së tyre (mundësi për paraqitje të kërcënimit).
4.4. Evaluim i rrezikut (kombinim i besueshmërisë për paraqitje të kërcënimit dhe ndikimi nga e njëjta).

pjesa 3: mjete për forcimin e pozicionit oficer për mbrojtjen e të dhënave personale

Që të forcohet dhe të përmirësohet efikasiteti i punës që e kryejnë oficerët për mbrojtjen e të dhënave personale dhe të intensifikohet bashkëpunimi me AMDHP, si dhe të vendosen forma të reja të bashkëpunimit mes oficerëve, është e nevojshme përpunimi i pakos të mjeteve, që vijojnë:

3.1. pako udhëzuesish

Ky Udhëzues është përpunuar si pjesë e tuining-projektit “Përkrahje në zbatimin e modernizimit të kornizës juridike për mbrojtjen e të dhënave personale”, financuar nga Bashkimi Evropian. Ai shërben si mjet për kryerje efikase të detyrave të oficerëve për mbrojtjen e të dhënave personale dhe përfshin informacione për risitë të cilat janë vendosur me legjislacion. Konkretisht, Udhëzuesi është i dedikuar për kuptim më të mirë të funksionit të tyre dhe për pozicionin e ri të kontrolluesve, dhe ofron sqarime për zbatim më të lehtë të detyrimeve. Pakoja e mjeteve të favorshme të përpunuara si pjesë e projektit përfshin numër më të madh të udhëzuesve, informatorë dhe dokumente të temave të ndryshme nga fusha e mbrojtjes së të dhënave personale, siç janë: të drejtat e subjektit të të dhënave personale; parimi i mbrojtjes së të dhënave personale; koncepti i kontrolluesit, përpunuesit dhe kontrolluesit të përbashkët, vlerësimi i ndikimit mbi mbrojtjen e të dhënave personale, bartjen e të dhënave në vende të treta dhe organizata ndërkombëtare, etj. Të arritshme në linkun si vijonlink.

3.2. rrubrika për oficerët

Deri tani bashkëpunimi me AMDHP është drejtuar në dhënien e këshillave të kontrolluesve t’i përmirësojnë operacionet e tanishme dhe të zhvillojnë praktika të mira në tema konkrete. Për intensifikimin e këtij bashkëpunimi, në faqen oficiale të ueb faqes të AMDHP duhet të vendosen rubrika për oficerë si formë e re e bashkëpunimit. Qasjate kjo pjesë e ueb faqes do të jetë e kufizuar vetëm për Agjencinë dhe oficerët.

Oficerë efikas janë vetëm ata të cilët janë mirë të informuar për dispozitat për mbrojtjen e të dhënave personale dhe janë në rrjedhë me progresin në këtë fushë. Rubrika do të shërbejë si platformë për këmbimin e njohurive dhe përvojave dhe për përkrahje në zbatimin e detyrave të tyre. Më konkretisht, oficerët do të kenë qasje te dokumentet e azhurnuara të cilat fokusohen në rolin e tyre dhe detyrat. Dokumentet do të jenë të dizajnuara në mënyrë që lejon pasqyrë të qartë dhe kuptim të shpejtë. Njëkohësisht, rubrika do të ofrojë përkrahje në zbatimin e detyrave të tyre, siç janë formularë dhe prezantime të cilat do të ndihmojnë ta forcojnë vetëdijen e të punësuarve te kontrolluesi ose përpunuesi ku punon oficeri.

Në mënyrë plotësuese, rubrika e oficerëve do të përfshijë pjesë ku do të sqarohen ngjarje vijuese (konferenca, seminare, trajnime dhe mbledhje) të cilat mund t’i vizitojnë që t’i plotësojnë me njohuritë dhe aftësitë e tyre, si dhe mjete tjera të cilat janë të nevojshme në punën e tyre të përditshme.

3.3. rrjeti i oficerëve

Për qëllimet e bashkëpunimit dhe këmbimit të përvojave mes oficerëve për mbrojtjen e të dhënave personale duhet të krijohet edhe rrjet i oficerëve. Duke pasur parasysh rëndësinë e interaksionit me kolegët, kurse në veçanti rëndësinë e ndarjes së praktikave të mira dhe këshillave praktike, rrjeti është mjet i favorshëm për informim më të mirë dhe punë efikase të oficerit.

Rrjeti i oficerëve mund të jetë pjesë e veçantë nga rubrika për oficerët ku ata do të kenë mundësi t’i identifikojnë kolegët e tyre. Ai duhet të dizajnohet në mënyrë e cila mundëson bashkëpunim të lehtë në përgjithësi, por edhe në nivel të sektorëve të posaçëm. Ky rrjet mund të jetë i favorshëm për dhënien e këshillave dhe këmbim të qëndrimeve për çështje të zakonshme dhe probleme.

Është e pëlqyeshme që në kuadër të rrjetit të formohen grupe të posaçme në nivel të sektorëve për bashkëpunim më të lehtë dhe këmbim të përvojave.

3.4. e- forume (e-konferenca)

Rekomandohet krijim i ueb mjeteve për organizim të e-forumeve (e-konferenca) të cilat do të mundësojnë komunikim mes oficerëve përmes shfrytëzimit të teknologjive më të reja të arritshme
Përmes këtij mjeti, oficerët për mbrojtjen e të dhënave personale do të kenë mundësi që në kohë të jenë të informuar për risitë në këtë fushë dhe të lëshohen në diskutime vijuese. E- Forumi do të krijojë tema të reja për çështje vijuese, kurse oficerët do të mund të bashkëngjiten në diskutimet dhe të këmbejnë qëndrime dhe përvoja për tema konkrete. Përveç kësaj, platforma duhet të mundësojë video komunikim të njëtrajtshëm, nga AMDHP drejt oficerëve, të cilët do mund të parashtrojnë pyetje në kohë reale.

3.5. shoqata e oficerëve

Edhe një formë e bashkëpunimit dhe këmbimit të njohurive dhe përvojave është formimi i shoqatës së oficerëve për mbrojtjen e të dhënave personale, nënkuptohet, me iniciativë të tyre.

3.6. programi i ri për trajnim të oficerëve

Që të forcohet pozicioni i oficerit, është e nevojshme të përpunohet program i ri për trajnim dhe materiale të reja në bazë të ligjit të ri të cilat do t’i shfrytëzojnë anëtarët e komisionit për trajnim në AMDHP. Materialet duhet të jenë të arritshme në formë elektronike dhe në letër, dhe të njëjtat duhet të përfshijnë hapa praktikë për plotësimin e detyrimeve nga legjislacioni i ri
Është e dëshirueshme që trajnimet të organizohen në nivel të sektorit, gjë që do ta lehtësojë implementimin e Ligjit të ri për mbrojtjen e të dhënave personale.

3.7. strategjia për komunikim

Strategjia për komunikim është mjet i rëndësishëm i cili përkrah zbatimin e legjislacionit të ri. Një pjesë nga strategjia për komunikim duhet të ketë të bëjë me rolin e ri të oficerëve për mbrojtjen e të dhënave personale. Përveç kësaj, ky dokument duhet të parasheh organizim të ngjarjeve publike dhe fushatave për ngritjen e vetëdijes dhe promovim të pozicionit të oficerit.

3.8. ditë të vetëdijes për rolin e oficerëbve

Rekomandohet organizimi i ditëve të vetëdijes për roline oficerëve për mbrojtjen e të dhënave personale si mjet për ngritjen e vetëdijes dhe për promovim të rolit të ri të oficerëve. Në këtë ngjarje duhet të ftohen udhëheqësit e organeve publike dhe drejtuesit e kompanive private që të njihen me profilin, pozicionin dhe detyrat e oficerit, si dhe kushtet dhe rrethanat në të cilat i kryejnë detyrat e tyre. Ngjarjet e tilla duhet të organizohen në bazë të rregullt.

Ky publikim është prodhuar me ndihmën financiare të Bashkimit Evropian. Përmbajtja e këtij publikimi është përgjegjësi vetëm e autorit dhe në asnjë mënyrë nuk mund të konsiderohet se pasqyron pikëpamjet e Bashkimit Evropian.

Kërkoni më shumë informacione në
www.azlp.mk

SCAN ME