МЕТАМОРФОЗИС
Фондација за интернет и општество

Rekomandime për Propozim-Strategjinë Kombëtare të TIK-ut 2021-2025 dhe Planin aksional shoqërues në lidhje me të drejtën për privatësi

(rekomandimet janë dhënë në kontekstin e zbatimit të Ligjit për Mbrojtjen e të Dhënave Personale (Gazeta Zyrtare e RMV nr. 42/20) dhe Rregullores së Përgjithshme për Mbrojtjen e të Dhënave Personale (GDPR-General Data Protection Regulation 2016/679)

- Në procesin e forcimit të kapaciteteve të TI-së të institucioneve, përveç profesionistëve të TI-së, një burim kyç njerëzor që duhet planifikuar seriozisht është edhe Zyrtari për Mbrojtjen e të Dhënave Personale. Roli i Zyrtarit për Mbrojtjen e të Dhënave Personale është ngritur në një nivel më të lartë ku ekspertiza dhe pavarësia janë në radhë të parë. Për të siguruar efikasitet në përmbushjen e detyrimeve, institucionet janë të detyruara të sigurojnë që Zyrtari për Mbrojtjen e të Dhënave Personale të përfshihet në mënyrë adekuate dhe në kohë në të gjitha çështjet që lidhen me mbrojtjen e të dhënave personale dhe t'i ofrojnë atij/asaj mbështetje në kryerjen e detyrave, duke ia siguruar të gjitha burimet e nevojshme dhe qasje në të dhënat personale dhe operacionet e përpunimit.

- Kur përcaktohet infrastruktura e qendrës qendrore të të dhënave të sigurta, veçanërisht në pjesën e shkarkimit të të gjitha aplikacioneve të të gjitha ministrive, agjencive, institucioneve, universiteteve dhe spitaleve, duhet të kihet parasysh se një numër i madh i aplikacioneve ekzistuese nuk i kanë të përfshira parimet për mbrojtjen e të dhënave personale. Çdo institucion që ka një aplikacion përmes të cilit përpunohen të dhënat personale duhet ta analizojë atë, ta vlerësojë atë dhe ta harmonizojë në mënyrë të detyrueshme funksionalitetet e tij me Ligjin për Mbrojtjen e të Dhënave Personale para se ta dorëzojë atë në qendrën e të dhënave. Koleksionet, aplikacionet dhe mjetet e tjera elektronike e paharmonizuara të të dhënave personale mund ta dobësojnë më tej sistemin e sigurisë dhe të mbrojtjes së të dhënave personale, dhe kështu ta rrezikojnë sigurinë e vetë qendrës qendrore të të dhënave.

- Ekziston një ndryshim thelbësor midis e-shërbimeve të institucioneve, të cilat janë një mënyrë alternative e marrjes së shërbimit (e jo shërbim shtesë të cilin qytetarët nuk do të mund ta merrnin ndryshe) dhe të atyre shërbimeve që janë të disponueshme për qytetarët vetëm në mënyrë elektronike (dhe të njëjtët qytetarët nuk mund t'i marrin në ndonjë mënyrë tjetër). Kjo është një çështje kryesore që duhet të merret parasysh patjetër në centralizimin e ofrimit të e-shërbimeve. Për shërbimet që janë të disponueshme për qytetarët vetëm në mënyrë elektronike, parimet e "vetëm një herë" dhe të përzgjedhjes së kanalit do të duhet të rishikohen dhe të rivlerësohet zbatimi i tyre.

- Miratimi i një strategjie komunikimi dhe planifikimi i aktiviteteve promovuese nuk duhet të detyrohen para se të kontrollohet më parë nëse shërbimet elektronike ekzistuese mbështeten nga Politikat e Privatësisë, nëse respektohen të gjitha parimet për mbrojtjen e privatësisë në ofrimin e shërbimit elektronik dhe nëse institucionet kanë përcaktuar mënyrën dhe kanalet përmes të cilave qytetarët mund të kërkojnë ushtrimin e së drejtës së tyre për privatësi.

- Qeveria duhet të sigurojë që puna e secilës ministri, organ, institucion, ndërmarrje publike që ofron shërbime elektronike është në përputhje me Ligjin për Mbrojtjen e të Dhënave Personale. Kjo veçanërisht për faktin se parimi i Sigurisë sipas dizajnit i referohet shërbimeve, mjeteve,

BE-ja me TY
Ky projekt është bashkë-financuar nga Bashkimi Evropian

ICEDA
Increasing Civic Engagement in the Digital Agenda

aplikacioneve të reja, e jo atyre ekzistuese të cilat pritet të ripërkufizohen në përputhje me parimet e Ligjit për Mbrojtjen e të Dhënave Personale.

- Qeveria duhet të sigurojë se çdo institucion që ofron shërbime elektronike t'i respektojë parimet e "ligjshmërisë, drejtësisë dhe transparencës"; "kufizimit të objektivave"; "vëllimit minimal të të dhënave"; "saktësisë"; "kufizimi të periudhës së ruajtjes"; "integritetii dhe konfidencialitetii" dhe "llogaridhënies".

- Në kontekstin e krijimit të një Qendre për internet më të sigurt për fëmijët, Qeveria duhet ta mbështesë procesin e transpozimit të Direktivës (BE) 2016/680 të Parlamentit Evropian dhe të Këshillit mbi mbrojtjen e individëve në lidhje me përpunimin e të dhënave personale nga autoritetet kompetente me qëllim të parandalimit, hetimit, zbulimit ose ndjekjes së veprave penale ose për zbatimin e sanksionet penale dhe për lëvizjen e lirë të këtyre të dhënave, e cila siguron përdorimin e mjeteve teknologjike nga policia që nuk e cenojnë privatësinë. Kjo Direktivë është dispozita e dytë kryesore, përveç Rregullores së Përgjithshme të Mbrojtjes së të Dhënave Personale (GDPR) në fushën e mbrojtjes së të dhënave personale, e cila duhet të jetë pjesë e legjislacionit kombëtar.

- Gjatë krijimit të e-shërbimeve ose mjete të reja, veçanërisht për shërbimet për ofrimin e të cilave nuk ka asnjë procedurë të përcaktuar ligjore (siç është, për shembull, StopCorona, vakcinacija.mk, TVSH-ja IME), Qeveria duhet t'i mbështesë institucionet në procesin e kryerjes së analizave dhe vlerësimit të ndikimit të privatësisë, si një hap i parë i detyrueshëm para se të merret vendim për ta krijuar e-shërbimin ose mjetin.

- Marrëdhënia midis Qeverisë dhe subjekteve të tjera duhet të përcaktohet qartë dhe duhet të dihet se cili subjekt në çfarë momenti shfaqet në rolin e përpunuesit të të dhënave personale, përdoruesit të të dhënave personale ose të palës së tretë. Kjo marrëdhënie duhet të rregullohet me marrëveshje të veçanta midis institucioneve, të cilat kanë të bëjnë ekskluzivisht me sigurimin e masave për mbrojtjen e të dhënave personale.

- Qeveria duhet të miratojë një metodologji për zbulimin, raportimin dhe korrigjimin e incidenteve të sigurisë që lidhen me shkeljet e sigurisë së të dhënave personale të qytetarëve gjatë përdorimit të e-shërbimeve ose mjeteve. Me këtë rast, qasja e sërishme në të dhënat që i janë nënshtruar incidentit duhet të sigurohet pa përjashtim.

- Agjencia për Mbrojtjen e të Dhënave Personale (AMDhP) duhet të përfshihet në mënyrë aktive në zbatimin e strategjisë së TIK-ut. Përveçse është një qendër burimore e njohurive dhe praktikave, AMDhP-ja do të duhet të japë mendimin, miratimin dhe udhëzimin e saj në një numër aktivitetesh, kështu që përfshirja e tyre është thelbësore për të siguruar një proces që do ta mbështesë zbatimin e Ligjit për Mbrojtjen e të Dhënave Personale në çdo aspekt.

Ky projekt është bashkë-financuar nga Bashkimi Evropian

ICEDA
Increasing Civic Engagement in the Digital Agenda