Aksion kontrolli i GPEN për vitin 2017 (GPEN *Sweep*) – Kontrollet e përdoruesit mbi informacionin personal

Hyrje

Aksioni i kontrollit të GPEN për vitin 2017 kishte për qëllim kontrollin e praktikave dhe komunikimeve të privatësisë lidhur me kontrollin e përdoruesit mbi informacionin personal. Faqet e internetit dhe aplikacionet celulare kanë potencialin për të mbledhur sasi të mëdha të të dhënave personale nga burime të ndryshme. Është e rëndësishme që përdoruesit të jenë të informuar për mënyrën se si të dhënat e tyre mblidhen, përdoren dhe shpërndahen. Tema "kontrollet e përdoruesit" lejon Agjencitë ligjzbatuese (PEAs) që marrin pjesë, të konsiderojnë nëse ishte e qartë nga perspektiva e përdoruesit se çfarë informacioni mblidhej ekzaktësisht nga faqja e internetit apo aplikacioni, qëllimi për të cilin ishte mbledhur dhe se si do të përpunohej, përdorej dhe shpërndahej ky informacion.

Një larmi metodologjish u përdorur në këtë aksion, përfshirë, por jo e limituar në:

- Kontrollin e komunikimeve të privatësisë që gjenden në faqe interneti/aplikacione – 21 Agjenci (PEAs);
- Krijimin e llogarive/profileve - 12 Agjenci (PEAs);
- Kontaktimin e zyrtarëve të privatësisë me një serë pyetjesh specifike – 3 Agjenci (PEAs).

Për të ngushtuar fokusin e kontrollit, Agjencitë (PEAs) u fokusuan në një sektor (sektorët) të veçantë, i cili përbënte rëndësi për to, përfshirë (por jo e limituar në);

- Arsim – 7 Agjenci (PEAs);
- Agjenci udhëtimi - 9 Agjenci (PEAs);
- Shitjet me pakicë - 9 Agjenci (PEAs);
- Shëndetësi - 4 Agjenci (PEAs);
- Rrjete sociale - 1 Agjenci (PEAs);
- Lojëra fati/kumari - 2 Agjenci (PEAs);
- Financë/veprime bankare - 4 Agjenci (PEAs);
- Të tjera - 2 Agjenci (PEAs).

Shënim: disa Agjenci kontrolluan në më shumë se një sektor.

Përmbledhje

Komunikimet e privatësisë në sektorë të ndryshëm, në përgjithësi, u gjetën në nivel shumë të lartë dhe nuk kishin detaje specifike. Gjithsesi, shpesh është vënë re nga Agjencitë (PEAs) se komunikimet e privatësisë gjenden lehtësisht në faqet e internetit dhe shumica e organizatave ishin mjaft transparente duke specifikuar se çfarë informacioni (apo kategori informacioni) mblidhnin.

Megjithatë, kontrolluesit në përgjithësi nuk arritën të specifikonin se me cilët palë do shpërndaheshin të dhënat. Nga kontrolli i Autoriteteve rezultoi, gjithashtu, se një numër kontrolluesish nuk arritën t'i jepnin detaje për çështjen e sigurisë së të dhënave të mbledhura dhe mbajtura nga ato; shpesh ishte e paqartë se ku arkivoheshin të dhënat (p.sh. në cilin shtet), apo nëse kishte ndonjë masë mbrojtëse për të garantuar të dhënat e përdoruesit. U konstatua, gjithashtu, se gjysma e organizatave të kontrolluara, referonin për mënyrën se si përdoruesit mund të aksesonin të dhënat personale që mbaheshin për ata. Kishte disa shembuj të praktikave të mira, por ishin të pakët në numër.

Gjetjet e përgjithshme sugjerojnë se përdoruesit (qytetarët) e shërbimeve të kontrolluara, në përgjithësi, nuk janë të informuar mirë se çfarë ndodh me të dhënat e tyre në momentin që mblidhen. Kështu përdoruesit nuk mund ta ushtrojnë lehtësisht të drejtën e kontrollit (aksesi, marrja dhe fshirja e të dhënave të tyre). Ekziston një hapësirë e konsiderueshme për përmirësim në lidhje me detajet specifike të përfshira në komunikimet e privatësisë.

Rezultatet e aksionit

Autoritetet e Mbrojtjes së të Dhënave që morrën pjesë: **24**

Faqe interneti/aplikacione të kontrolluara: **455**

***Shënim metodologjie**: jo të gjithë Autoritetet njoftuan mbi çdo fushë raportuese. Statistikat për këtë aksion kontrolli u zhvilluan në bazë të të dhënave aktuale, të marra për një fushë raportimi si një përqindje e faqeve të internetit/aplikacioneve të kontrolluara nga ato Autoritete që raportuan mbi atë fushë.*

Mbledhja dhe përdorimi i të dhënave (Indikatori 1)

Autoritetet që morrën pjesë në aksionin e kontrollit treguan se rreth **23%** e website-ve/aplikacioneve nuk specifikonin saktësisht në komunikimet e tyre të privatësisë se çfarë informacioni do të mblidhej nga përdoruesi, ndërkohë që rreth **17%** nuk merrnin pëlqimin e duhur për të mbledhur këto të dhëna.

Bazuar në komunikimet e privatësisë që gjenden në website/aplikacion, përdoruesit ishin të informuar se informacioni që vijon (plus informacione të tjera) do të mblidheshin qoftë me detyrim apo mbi baza opsionale nga organizatat e kontrolluara:

- emri: 81% e *web*/app;
- ditëlindja: 52% e *web*/app;
- adresa: 51% e *web*/app;
- numri i telefonit: 45% e *web*/app;
- adresa *e-mail*: 85% e *web*/app;
- të dhënat e përdorimit: 38% e *web*/app;
- multimedia (audio/video/foto): 8% e *web*/app;
- vendndodhja: 16% e *web*/app;
- informacion mbi palët e treta: 9% e *web*/app;
- të dhëna biometrike: 3% e *web*/app;
- detaje financiare: 25% e *web*/app;
- informacion shëndetësor: 5% e *web*/app;
- adresat IP: 69% *web*/app.

Trendet lidhur me Indikatorin 1

- Sektori privat parashikonte dhënien e pëlqimit në komunikimet e privatësisë më shumë se sektori publik, ku këta të fundit mbështeteshin në autoritetin e tyre ligjor për të mbledhur

informacionin.

- Në shumë raste, politikat e privatësisë referonin shpesh në të dhëna (apo kategori të dhënash) që mund të mblidhen.
- Informacion për mënyrën se si të dhënat personale do të përdoreshin ishte shpesh i përgjithshëm.
- Disa *faqe*/aplikacione nuk bënin referencë për mbledhjen e informacionit nëpërmjet *cookies*, pavarësisht se e mblidhnin këtë informacion në praktikë.
- Shumë faqe mbledhin informacion në baza *opt-out,* duke u mbështetur në pëlqimin e nënkuptuar (për shembull: nëse përdorni këtë faqe ju jepni pëlqimin tuaj për mbledhjen dhe përpunimin e informacionit tuaj).
- Në shumë raste, politikat e privatësisë përdornin një strukturë të shtresuar, duke i bërë të qarta dhe të thjeshta për përdoruesit.
- Përveç një politike të shkruar të privatësisë, disa *faqe* shfaqnin një video, për t'i shpjeguar politikat e privatësisë në gjuhë të thjeshtë dhe të qartë.

Arkivimi dhe siguria e të dhënave (Indikatori 2)

Bazuar në gjetjet e kontrollit, vetëm 35% e faqeve/aplikacioneve specifikuan në komunikimet e tyre të privatësisë nëse ato kanë vendosur ndonjë masë mbrojtëse për të garantuar sigurinë e të dhënave të përdoruesit (si kontroll aksesi, enkriptimi, etj.).

Nga faqet/aplikacionet e kontrolluara, 67% nuk specifikonin se ku arkivohen të dhënat (p.sh. në cilin shtet).

Trendet lidhur me Indikatorin 2

- Ekziston një trend i përgjithshëm (në gjithë sektorët) ku komunikimet e privatësisë nuk i këshillonin përdoruesit për mënyrën se si apo ku të dhënat e tyre do të arkivohen.
- Disa faqe akoma bazoheshin në 'Safe Harbor' (marrëveshja e vjetër për transferimin e të dhënave të qytetarëve të BE në SHBA), e cila u shpall e pavlefshme nga Gjykata Evropiane e Drejtësisë në tetor 2015.

Shpërndarja e të dhënave (Indikatori 3)

Në këtë aksion kontrolli rezultoi se 51% e faqeve/aplikacioneve nuk specifikuan se me kë duhet të ndahen të dhënat, ndërkohë që 25% nuk përmendnin nëse informacioni personal do të përhapej tek palët e treta.

Trendet lidhur me Indikatorin 3

- Shpesh ishte e paqartë se me kë palë të treta do të shpërndaheshin të dhënat dhe shumë faqe nuk përmendnin se ato i ndajnë të dhëna.
- Organizatat ishin në përgjithësi të paqarta se çfarë informacioni do të shpërndahej.
- Detajet rreth transferimit ndërkombëtar të të dhënave ishin të paqarta. Për shembull, shumë organizata informonin se të dhënat mund të 'transferoheshin jashtë Zonës Ekonomike Evropiane', por nuk specifikonin se ku apo se për çfarë qëllimi.

Fshirja e të dhënave (Indikatori 4)

Rreth 51% e faqeve/aplikacioneve japin udhëzime se si mund të hiqen të dhënat personale nga data-baza e tyre në komunikimet e privatësisë.

Vetëm 22% specifikonin nëse ishte vendosur një politikë mbajtjeje të të dhënave, ndërkohë që shumica dërrmuese e faqeve/aplikacioneve të kontrolluara nuk japin ndonjë shpjegim se çfarë ndodh me llogaritë e fjetura/joaktive.

Aksesi i të dhënave të përdoruesit (Indikatori 5)

Autoritetet e përfshira në këtë aksion vunë re se 56% e faqeve/aplikacioneve u bëjnë të qartë përdoruesve se si ata mund të aksesonin të dhënat e tyre personale.

Vendimmarrja automatike (Indikatori 6)

Rreth 39% e organizatave specifikuan se disa vendime do të bëheshin

me anë të mjeteve automatike; e ku 23% e tyre vënë në dukje se si përdoruesi mund të kundërshtojë një vendim në të tilla rrethana apo të kërkojë ndërhyrjen njerëzore.

Konstatime të tjera

- Disa organizata/kontrollues u referoheshin legjislacioni të vjetruar.
- Një numër organizatash që ofrojnë shërbime në nivel ndërkombëtar ishin të paqarta lidhur me zbatueshmërinë juridiksionale apo legjislative.
- Është vërejtur se shitësit me pakicë që lëshojnë raporte elektronike, në përgjithësi nuk arritën të japin ndonjë informacion në lidhje me faturat në faqet e tyre të internetit.
- Në përgjithësi vihet re se faqet e bankave nuk mbanin shumë detaje në politikën e tyre të privatësisë. Sidoqoftë, politikat shpesh herë theksuan se si detajet e mëtejshme për përdorimin dhe mbledhjen e të dhënave mund të gjendeshin gjatë plotësimit të formularit të regjistrimit, apo në kushtet dhe kriteret përkatëse të ofruara për konsumatorët.

Konkluzione

Në mënyrë të përmbledhur, komunikimet e privatësisë në sektorë të ndryshëm prireshin të ishin të paqartë dhe shpesh, përmbanin klauzola të përgjithshme. Shumica e organizatave nuk informonin përdoruesin se çfarë do të ndodhte me informacionin e tyre në momentin që ai jepej.

Është e rëndësishme që përdoruesit të kenë të qartë se si të kontrollojnë informacionin e tyre në internet. Është e vështirë për një përdorues që të ushtrojë kontrollin e tij kur nuk është i informuar për mënyrën që duhet të ndjekë për ta bërë këtë. Bazuar në gjetjet e lartpërmendura, përdoruesit duhet të jenë të informuar më mirë lidhur me mënyrën se si duhet të aksesojnë apo heqin informacionin që ata japin në internet, nëse informacioni do të shpërndahet dhe se me kë, si dhe nëse informacioni që ata japin do të arkivohet në një mënyrë mjaft të sigurt.