Scripture Union International

Udhëzues për

Stafin

Përdorimi i të dhënave personale

Pasqyra e Lëndës

1. Hyrje

Akti për Mbrojtjen e të Dhënave i vitit 2018 (‘DPA’) rregullon përdorimin e të dhënave personale nga organizatat me bazë në Mbretërinë e Bashkuar (‘MB’). Ai hyri në fuqi më 23 maj 2018 dhe zbaton standardet e BE-së për mbrojtjen e të dhënave personale siç përcaktohen në Rregulloren e Përgjithshme të Mbrojtjes së të Dhënave ('GDPR'), megjithëse me disa rregullime teknike ("përjashtime") që modifikojnë zbatimin e GDPR-së në MB.

DPA përcakton rregullat për qeverisjen se si SUI si një organizatë, mund t’i përdorë të dhënat personale. Qëllimi i këtij dokumenti është të sigurojë udhëzime për stafin në lidhje me procedurat e zbatimit të cilat mbështesin dhe sigurojnë pajtueshmërinë e SUI rreth DPA-së.

Konkretisht, DPA kërkon që ne:

• T’i përdorim të dhëna personale vetëm atje ku na duhet dhe të përdorim vetëm minimumin e kërkuar për përmbushjen e objektivave tona;
• Të jemi transparentë në lidhje me mënyrën dhe arsyjen e përdorimit të dhënave personale;
• Të kemi një bazë të ligjore për përdorimin e këtyre të dhënave;
• Të kemi sisteme funksionale të duhura për korrigjimin e të dhënave të pasakta personale dhe mbajtjen e tyre të përditësuara;
• Të kemi sisteme funksionale për shkatërrim të sigurt të të dhënave atëherë kur nuk na duhen më;
• Të zbatojmë masat e duhura të sigurisë që mbrojnë të dhënat personale; dhe
• Të mos transferojmë të dhënat personale jashtë BE-së nëse nuk ekzistojnë aranzhime shumë specifike të përshtatshmërisë.

Vini re se DPA-ja është krijuar për të mbrojtur të dhënat personale të qytetarëve të BE-së. Rrjedhimisht, edhe nëse jeni duke punuar jashtë shtetit, brenda komunitetit më të gjerë botëror të Scripture Union, është e rëndësishme të pranoni që aktivitetet tuaja mund të mbulohen nga DPA nëse jeni duke procesuar – d.m.th. po përdoroni – të dhëna personale të një individi nëse ai individ ishte banor në BE kur u mblodhën të dhënat. P.sh. kjo mund të përfshijë adresat personale të financuesve të programeve.

Jini të vetëdijshëm se nën DPA të dhënave e ndjeshme personale u ofrohet një nivel edhe më i lartë i mbrojtjes. Të dhënat e ndjeshme personale janë informacione në lidhje me racën, etninë, kryerjen e një vepre penale të një individi (ose faktin që ata i janë nënshtruar procedurave penale), mendimet politike, besimet fetare dhe anëtarësimin e tyre në një sindikatë.

DPA është përgjithësisht shumë më e rreptë se legjislacioni i mëparshëm – në fuqi që nga viti 1998 – për sa i përket kohës kur mund të përdorim të dhëna personale, çfarë duhet t'u tregojmë individëve se si i përdorim ato dhe sa shpejt duhet të përgjigjemi në rast të një shkeljeje me të dhëna personale (shih seksionin 9 për udhëzime të mëtejshme). Veprat penale dhe ndëshkimet e rënda financiare të përcaktuara në GDPR përfshihen në DPA. DPA gjithashtu kërkon që ne të demonstrojmë se si të sillemi në përputhje me Rregulloren dhe të vendosim gjoba më të rrepta për mosrespektim. Ju mund të lexoni më tepër se si ka reaguar SUI lidhur me udhëzimet për Politikën për Mbrojtjen e të Dhënave të SUI.

2. Struktura për qeverisjen e informacionit

Politika e Mbrojtjes së të Dhënave e SUI përcakton me hollësi se si ne si organizatë i përmbahemi DPA-së. I gjithë stafi është përgjegjës për t'ju përmbajtur Politikës për Mbrojtjen e të Dhënave të SUI dhe të gjithë menaxherët janë përgjegjës për të siguruar që stafi që u raporton stafit të ndjekë politikat, proceset dhe udhëzimet e Mbrojtjes së të Dhënave të SUI. Në praktikë, kjo do të thotë që menaxherët duhet ta ndërgjegjësojnë stafin e tyre rreth Politikës për Mbrojtjen e të Dhënave dhe kur është e përshtatshme, të këshillojnë stafin se ku dhe kur duhet të ndiqen ato procese. Në një nivel ekzekutiv, Bordi Ndërkombëtar i i Scripture Union mban në mënyrë të ngjashme përgjegjësinë për promovimin e këtyre politikave dhe proceset në të gjithë organizatën dhe në fund të fundit është përgjegjës për çdo shkelje.

3. Mbledhja dhe përdorimi i të dhënave personale

3.1 Minimizimi i të dhënave

- Merrni parasysh nëse keni nevojë për ndonjë të dhënë personale të mbajtur për të arritur objektivin tuaj.

P.sh., kur vendosni ta rishikoni efikasitetin dhe përshtatshmërinë e kanaleve të financimit. mund të duhet të mbledhësh të dhëna personale nga besimet, fondacionet dhe donatorët të ndërmarrë këtë analizë. Sidoqoftë, pasi të dhënat janë analizuar dhe statistikat janë analizuar të përgatitur mund të mos jetë më e nevojshme të ruhen të dhënat personale në mënyrë që kryej rishikimin. Në atë rast, informacioni i identifikueshëm (p.sh. emrat e dhuruesve dhe adresat e postës elektronike) duhet të hiqen nga informacioni statistikor.

- Mblidhni ose përdorni vetëm sasinë minimale të të dhënave personale të nevojshme për objektivat specifike të biznesit tuaj.

P.sh. për të administruar një skemë të grantit për arsim, mund t'ju duhet të mblidhni emrat e individëve, adresat dhe numrat e maturimit të studentëve, por nuk do të keni nevojë të grumbulloni lloje të tjera të të dhënave personale të tilla si mosha ose etnia.

3.2 Transparenca

- Sigurohuni që njerëzit janë të njoftuar lidhur me mënyrën dhe arsyjen e grumbulimit të dhënave të tyre personale, kohëzgjatjen e ruajtës së atyre të dhënave, me kë i ndajmë ato, përgjegjësitë e SU-së sipas DPA-së dhe të drejtat e tyre në lidhje me të dhënat e tyre në përputhje atë Ligj ('informacion i procesimit të drejtë'). Kjo duhet të bëhet në njoftim të SU-së për procesimin e duhur e të dhënave të cilën e ndan Drejtori Ndërkombëtar.

- Në rast se arsyeja juaj për përdorimin e të dhënave personale nuk është adresuar në Njoftimin për procesimin e duhur e të dhënave, kontaktoni menaxherin tuaj ose Drejtorin Ndërkombëtar i cili mund të sigurohet që njoftimi të përditësohet ose të këshilloni për metodat alternative për komunikim.
- Në rast se keni nevojë ta shpërndani Njoftimin për procesimin e duhur e të dhënave për një shërbim ose qëllim shumë specifik (të tilla si një sondazh në internet ose një faqe rekrutimi), ju lutemi kontaktoni Drejtorin Ndërkombëtar i/e cili do të sigurohet që t'ju dhurohet një njoftim shabllon për porosinë e porositur.

4. Shpalosja e brendshme

- Të dhënat personale të ndahen vetëm me ato skuadra që kanë një nevojë të mirëfilltë biznesi për qasje në të dhënat personale.
- Ndani vetëm sasinë minimale e të dhënave personale që atyre skuadrave u nevojitet për përmbushjen e objektivit të tyre biznesor.
- Nëse planifikoni që të dhënat personale t'i ndani me një skuaër në baza rutinore dhe këtë nuk e keni bërë më parë, informoni Drejtorin Ndërkombëtar për qëllimet tuaja. Nëse ju ose menaxheri juaj keni shqetësime në lidhje me ndarjen e atyre të dhënave personale, atëherë kontaktoni Drejtorin Ndërkombëtar për këshilla.
- Sigurohuni që keni zbatuar një metodë të sigurt për ndarjen e të dhënave personale me skuadrat tuaja.

Për shembull, nëse keni nevojë që rregullisht të ndani vëllime të mëdha të të dhënave ose të dhëna personale të ndjeshme me një skuadër tjetër, mund të krijoni një dosje të përbashkët në sistemet e vetë SU-së. Ju do të duhet të kufizoni qasjen tek individët e duhur. Si alternativë, ju mund të aplikoni mbrojtje me fjalëkalim në dokumentin që përmban të dhënat personale. Fjalëkalimi duhet të dërgohet veçmas nga dokumenti.

- Nëse jeni një ekip i tërë që merr të grumbullimin e të dhënave personale, duhet ta keni parasysh nëse individët janë informuar për përdorimin e synuar të të dhënave (shih pjesën e transparencës më lart).
- Në rast se të dhënat do t'i përdorni për një qëllim krejtësisht të ri, duhet të kryni një studim të prapavisë të Vlerësimit të Ndikimit të Privatësisë për të identifikuar nëse duhet të ndërmerret një Vlerësim i Ndikimit të Privatësisë. Kontaktoni Drejtorin Ndërkombëtar për udhëzime.

5. Shpalosja e jashtme

5.1 Shpalosjet Ad-hoc

- Skuadrat mund të pranojnë shumë kërkesa prej organizatave të jashtme për t'ju zbuluar atyre të dhëna personale.
- Skuadrat mund t'i zbulojnë të dhënat personale ndonjë organizate të jashtme vetëm pas pranimit të pëlqimit të individit për ta bërë këtë ose kur ekziston një bazë tjetër ligjore për shpalosjen e të dhënave.

P.sh. ju mund të pranoni ndonjë kërkesë nga Policia që kërkon informacione lidhur me një vullnetar në kontekstin e një hetimi penal. Në rast se merrni një kërkesë të tillë, luteni ta kontaktoni Drejtorin Ndërkombëtar i cili do ta mbikëqyrë procesin e shpalosjes së të dhënave duke e shqyrtuar kërkesën për të siguruar që ekziston një bazë ligjore për zbulimin dhe ndërlidhjen direkt me policinë.

- Nëse jeni të kënaqur që keni marr pëlqimin e një individi për t'i shpalosur të dhënat e tij ose ekziston një bazë tjetër ligjore për të bërë zbulimin e atyre të dhënave, para se të zbuloni të dhënat personale sigurohuni që e keni hulumtuar identitetin e parashtruesit të kërkesës.

P.Sh. nëse keni marrë një telefonatë që kërkon zbulimin e të dhënave personal, ju mund t'i kërkoni parashtruestit të kërkesës që t'ju dërgojë një email për ta verifikuar identitetin e tyre. Ju duhet të kontrolloni adresën e postës elektronike për të kontrolluar se është një adresë e njohur e lidhur me atë organizatë. Sigurisht që duhet të kontrolloni adresat e emailit që janë adresa të njohura para se të zbuloni të dhënat personale. Nëse nuk jeni të sigurt, duhet të kontaktoni Drejtorin Ndërkombëtar.

5.2 Shpalosjet e rregullta

- Nëse jeni duke kontraktuar një organizatë të jashtme në emër të SU-së për ofrim shërbimesh, do të duhet të lidhni një kontratë me atë organizatë duke këmbëngulur për masa specifike të atilla si kërkesa që kontraktori është përgjegjës për masat e duhura të sigurisë për mbrojtjen e të dhënave.
- Në rast se rregullisht po ndani të dhëna personale me një organizatë tjetër dhe nuk po e paguani atë organizatë për një shërbim, atëherë mund të jetë e nevojshme të lidhni një marrëveshje për "ndarjen e informacionit". Një marrëveshje për ndarjen e informacionit duhet të ekzistojë gjithmonë nëse ndani vëllime të mëdha të të dhënave ose të dhëna me një ndjeshmëri të veçantë (të tilla si informacion mjekësor ose informacion në lidhje me veprat penale). Ju lutemi flisni me Drejtorin Ndërkombëtar i cili do t'ju këshillojë.
- Çdo skuadër duhet të mbajë një listë të organizatave me të cilat ata ndajnë rregullisht të dhëna personale duke përfshirë kontraktorët, organizatat e kolegëve, organet qeveritare, autoritetet publike etj.

- Skuadrat duhet t'i rishikojnë rregullisht këto lista (p.sh. në baza tremujore) për të vlerësuar nëse po ndani të dhëna me organizata të reja ose nëse duhet përditësuar kontratat ose marrëveshjet ekzistuese me këto organizata.

6. Përditësimi i të dhënave personale

- Për aq sa është e mundur, skuadrat duhet të zbatojnë procedura që u mundësojnë individëve t'i përdotësojnë me lehtësi dhe shpejt të dhënat e tyre personale aty ku duhet të azhurnojnë informacione të tilla si një ndryshimi i adresës.

P.sh. vullnetarëve që kthehen për një kamp të SU-së duhet t'u kërkohet përtërirja e regjistrimit të tyre çdo vit, duke përfshirë plotësimin e një pyetësori i cili u kërkon atyre të përditësojnë detajet e tyre të kontaktit nëse janë të vjetruara.

- Skuadrat duhet t'i kenë të qarta përgjegjësitë e secilit pjesëtar të stafit rreth përditësimt e të dhënave personale kur të dhënat janë të pasakta ose të vjetruara.

Shembull: në një kontekst të shërbesës me sportistë – p.sh., kur kërkohet regjistrimi për një program të aktiviteteve të përsëritura çdo sezon – menaxherët mund të vendosin që punonjësit e veçantë të projektit janë përgjegjës për përditësimin e të dhënave kur ndryshimet në rrethana të pjesëmarrësve janë këshilluar.

7. Siguria e informacionit

- Informacioni që lihet pa mbikëqyrje ka më shumë të ngjarë të vidhet, të shpaloset gabimisht ose t'i zbulohet personit të gabuar. Për të ndihmuar në mbrojtjen e informacionit, stafi duhet të ç'kyçë ekranet e kompjuterit të tyre kur largohen nga tryezat e tyre për të shmangur shikimin e informacionit të ndjeshëm nga të tjerët.
- Stafi duhet gjithashtu të sigurojë që të gjitha dokumentet e ndjeshme të printuara të ruhen në hapësira të mbyllura – një sirtar i mbyllur do të ishte e mjaftueshme – në fund të çdo dite pune, ose sa herë që do të mbetet pa mbikëqyrje për një kohë të pacaktuar.
- Zgjidhni një fjalëkalim të sigurt që i plotëson standardet e industrisë – sa më i gjatë aq më i mirë, që përmban një përzierje të llojeve të karaktereve (shkronja të vogla, të mëdha, shenjat e pikësimit dhe numera). Duhet të jetë ndryshe nga 12 fjalëkalimet tuaja të fundit, kompleks por që mund të mbahet mend.
- Asnjëherë mos ndani fjalëkalimin tuaj me askënd tjetër. Nëse besoni se fjalëkalimi juaj nuk është më privat, ju lutemi ndryshojeni atë menjëherë dhe njoftojeni menaxherin tuaj se e keni bërë këtë.
- Ruani të dhënat personale vetëm në sistemet dhe pajisjet e aprovuara nga SU. Në mënyrë ideale, ruani të dhënat personale në vetë sistemet e bazuara në "cloud" të SU-së (të tilla si DropBox).

- Nëse keni ndërmend të përdorni një sistem tjetër të bazës “cloud” për të ruajtur të dhënat personale, atëherë duhet të kontrolloni që kontrollet e sigurisë për atë sistem janë të përshtatshme. Nëse nuk jeni të sigurt për një sistem që përdorni aktualisht, ju lutemi kontaktoni hostin dhe vendosni standardet që po aplikohen.

8. Mbajtja dhe shkatërrimi i sigurt

- Stafi do të duhet të përcaktohet periudhën e përshtatshme të mbajtjes së të dhënave personale që ata mbajnë dhe pastaj të mbajnë një regjistër për sa kohë kanë ruajtur secilën artikull të të dhënave personale. Stafi duhet t'i referohet Politikës së Mbrojtjes së të Dhënave të SUI, e cila përcakton periudhat e mbajtjes së SUI që rekomandon për llojet e regjistrimeve që mban aktualisht; nëse nuk mendoni se të dhënat personale që mbani janë të mbuluara në këtë orar, ju lutemi kontaktoni Drejtorin Ndërkombëtar dhe të bini dakord për një afat të përshtatshëm të mbajtjes.
- Drejtuesit e skuadrave duhet t'ia bëjnë të qartë personelit të tyre se kush ka përgjegjësi për shkatërrimin e shënimeve të veçanta kur skadon periudha e mbajtjes së atyre shënimeve. Drejtuesit e skuadrave duhet të kërkojnë nga stafi të raportojë rregullisht për të konfirmuar që të dhënat janë shkatërruar brenda këtyre afateve.
- Të dhënat personale duhet të shkatërrohen në një mënyrë të përshtatshme e të sigurt. Të dhënat personale në regjistrat e kopjuar duhet të hidhen në koshat konfidencialë të mbeturinave. Skuadrat nuk duhet të hedhin kurrë të dhëna personale në koshat e zakonshëm të mbeturinave.
- Email-et mund të fshihen duke zgjedhur fshirjen dhe zbrazjen e dosjeve tuaja të artikujve të fshirë. Do të ketë funksione të ngjashme për fshirjen e regjistrave elektronikë në sistemet e tjera të ruajtjes së regjistrave elektronikë të SUI. Nëse hasni vështirësi në fshirjen e të dhënave tuaja elektronike, ju lutemi kontaktoni Drejtorin Ndërkombëtar.
- Kur bleni sisteme të reja të teknologjisë së informacionit për ruajtjen e të dhënave personale, stafi duhet ta ketë parasysh faktin nëse sistemi mund të projektohet për të fshirë regjistrimet pasi të ketë skaduar një periudhë e veçantë e mbajtjes. Kur sigurohen sisteme të reja të TI-së, duhet të ndërmerret një Vlerësim i Ndikimit të Privatësisë. Kjo do të ndihmojë në identifikimin e kërkesave funksionale (të tilla si automatike fshirja) që mund të ndihmojë në mbështetjen e pajtueshmërisë së Mbrojtjes së të Dhënave.

9. Të drejtat e pronarit e të dhënave

- Subjektet e të dhënave kanë një sërë të drejtash në lidhje me të dhënat e tyre personale duke përfshirë të drejtat për qasje në të dhënat e tyre personale; të kërkojë që të dhënat personale të fshihen;
- Nëse merrni një kërkesë nga një individ për të ushtruar një nga të drejtat e mësipërme, atëherë do të duhet të informoni Drejtorin Ndërkombëtar sa më shpejt të jetë e mundur i cili do të këshillojë dhe ofrojë ndihmën e bashkërendimit të përgjigjes nga SUI. Informacioni mund të mbahet në shumë vende. Ekzistojnë afate kohore të rrepta për respektimin e të drejtave të mësipërme (40 ditët e kalendarit është maksimumi) prandaj ju lutemi mos vononi në kontakt.

- Kur kontaktoni Drejtorin Ndërkombëtar, ju lutemi merrni parasysh nëse skuadrat e tjera mund të kenë qasje në të dhënat personale të një individi dhe mund të kenë nevojë të informohen për një kërkesë të tillë.

10. Keqpërdorimi i të dhënave personale

Keqpërdorimi i të dhënave personale nënkupton shkeljen e sigurisë që çon në shkatërrim, humbje, ndryshim, zbulim të paautorizuar i të dhënave personale. Të dhënat nënkuptojnë informacione në çdo formë duke përfshirë shënime letre, posta elektronike, fakse etj. Shembuj të shkeljeve të të dhënave personale mund të përfshijnë përcjelljen e një tabele e të dhënave vullnetare te një marrës i paqëllimtë (i jashtëm ose i brendshëm), ose një vjedhje e dokumenteve delikate të lëna në një dhomë të zhbllokuar. Shkeljet personale duhet t'i raportohen Drejtorit Ndërkombëtar menjëherë; nëse vjedhja përfshin një pajisje të lëvizshme ose IT, veprimi i duhur duhet gjithashtu të ndërmerret drejtpërdrejt me furnizuesin e pajisjeve ose mikpritësin e komunikimit.

- Nëse e dini ose dyshoni se mund të ketë ndodhur një shkelje e të dhënave personale, kontaktoni Drejtorin Ndërkombëtar, i cili do t'ju kërkojë detaje në lidhje me rrethanat e shkeljes, llojin e të dhënave të përfshira dhe me të cilat lidhen ato të dhëna dhe ndikimin e mundshëm mbi individët e prekur.

- SUI duhet të mbajë një regjistër të të gjitha shkeljeve të të dhënave personale, pavarësisht nga ashpërsia; kështu që të gjitha shkeljet - ose shkeljet e dyshuara - duhet t'i njoftohen Drejtorit Ndërkombëtar. Për më tepër, nëse të drejtat ose liritë e subjektit mund të rrezikohen si rezultat i shkeljes, atëherë SUI duhet gjithashtu të raportojë shkeljen tek rregullatori, Zyra e Komisionarit të Informacionit dhe do t'i nënshtrohet një afati kohor të rreptë 72 orësh në të cilin për ta bërë këtë. SUI mund të gjobitet rëndë për mos raportim brenda periudhës.

- Mos harroni se afati 72-orësh fillon nga momenti kur ndonjë individ brenda organizatës zbulon se ka ndodhur shkelja e të dhënave personale – jo kur është raportuar tek Drejtori Ndërkombëtar.