Univerza v Ljubljani
Fakulteta za računalništvo in informatiko

Maja Umek

Splošna uredba o varstvu podatkov (GDPR) in podatkovno intenzivne mobilne aplikacije

diplomsko delo

interdisciplinarni univerzitetni
študijski program prve stopnje
računalništvo in matematika

Mentor: izr. prof. dr. Matjaž Kukar

Ljubljana, 2018

Besedilo je oblikovano z urejevalnikom besedil LaTeX.

Fakulteta za računalništvo in informatiko izdaja naslednjo nalogo:

Tematika naloge:

Uredba GDPR prinaša nove zahteve, ki jih morajo upoštevati razvijalci spletnih in mobilnih aplikacij, predvsem tistih, ki intenzivno zbirajo ali upravljajo z osebnimi podatki. Preglejte zahteve GDPR in glede na njih aplikacije sistematično razdelite v kategorije. Upoštevanje uredbe ilustrirajte na primeru razvoja GDPR-skladne mobilne aplikacije za sistem Android.

Kazalo

Seznam uporabljenih kratic

kratica	pomen
AES	Advanced Encryption Standard
API	Application Programming Interface
CRUD	Create, Read, Update, Delete
CSV	Coma-separated Value File Format
EU	Evropska unija
GDPR	General Data Protection Regulation
GPS	Global Positioning System
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
ID	Identifier
JSON	JavaScript Object Notation
JWT	JSON Web Token
MIME	Multipurpose Internet Mail Extension
REST	Representational State Transfer
SQL	Structured Query Language
URL	Uniform Resource Locator
XML	Extensible Markup Language
ZVOP	Zakon o varstvu osebnih podatkov

Povzetek

Naslov: Splošna uredba o varstvu podatkov (GDPR) in podatkovno intenzivne mobilne aplikacije

Avtor: Maja Umek

Uredba GDPR je prinesla kar nekaj novih zahtev, ki jih morajo upoštevati tudi mnogi razvijalci mobilnih aplikacij. Ti zbirajo osebne podatke posameznikov, ki pred veljavo GDPR niso imeli točnih informacij o tem, katere podatke vse o njih hranijo in obdelujejo razni ponudniki storitev. V diplomskem delu pregledam zahteve GDPR in jih implementiram na primeru Android mobilne aplikacije, ki se jih zaradi podatkov, ki jih obdeluje, mora držati. Aplikacijo glede na to, kaj vse mora upoštevati uvrstim v pripadajoče kategorije, določene na podlagi obsega zahtev, ki jih mora neka aplikacija izpolnjevati.

Ključne besede: GDPR, osebni podatki, mobilna aplikacija, Android.

Abstract

Title: General Data Protection Regulation (GDPR) and data-intensive mobile applications

Author: Maja Umek

GDPR has brought quite a few new requirements that many mobile application developers have to comply with as well. They collect personal data of individuals, who had no information on which of their data was stored and processed by various service providers before the enforcement of GDPR. In this diploma thesis, I go over the requirements of GDPR and implement them on a case of Android mobile application, that has to be GDPR compliant due to the data it processes. Based on the requirements that need to be met, I place the application into corresponding categories, defined by the scope of GDPR requirements that a certain application has to meet.

Keywords: GDPR, personal data, mobile application, Android.

Poglavje 1

Uvod

Ljudje danes premalo vemo o tem, kam vse se posredujejo naši osebni podatki, kdo jih obdeluje, s kakšnim namenom, itd. Informacijska tehnologija je v zadnjih letih močno napredovala in skupaj z globalizacijo omogočila zbiranje ogromnega števila osebnih podatkov, katerih izmenjava je postala precej preprosta. Hkrati z napredkom smo izgubili sledljivost naših osebnih podatkov, ki se uporabljajo tako v zakonite kot nezakonite namene. Zavedati se moramo, da se na podlagi naših podatkov velikokrat ustvarjajo uporabniški profili. Profiliranja se je večina nekoliko že navadila, zato ljudi ne zaskrbi, ko jim spletne strani prikažejo prilagojeno vsebino. Nekaterim se morda celo dobro zdi, ko jim nekdo ponuja ravno tisto, kar trenutno iščejo, ne pomislijo pa na to, da se na podlagi teh profilov lahko sprejemajo tudi odločitve, ki za njih niso ugodne. Spletna trgovina uporabniku lahko ne prikaže izdelkov, za katere se glede na kupčeve podatke odloči, da niso v njegovem cenovnem rangu. O avtomatiziranih odločitvah torej morda niti ne vemo. Nad svojimi osebnimi podatki je zato dobro imeti nadzor.

GDPR (General Data Protection Regulation) ali Splošna uredba o varstvu podatkov [7], v nadaljevanju „uredba“, je po svetu dvignila precej prahu. Zahteve uredbe so obširne in so večini velikih kot tudi malih podjetij in organizacij prinesle veliko dela, med drugimi tudi zato, ker ta kljub dosedanjim zakonom niso izvajala dovolj varnostnih ukrepov za pravice posameznikov.

Z neposredno veljavo uredbe, ki je prinesla visoke kazni v primeru njenega kršenja, pa so bila prisiljena delovati po njenih pravilih. Vendarle pa uredba ne zadeva le velikih podjetij in organizacij, pač pa tudi posamezne razvijalce mobilnih aplikacij. Skoraj vsaka mobilna aplikacija na nek način zbira podatke o posameznikih. To so lahko podatki o lokaciji, osebni podatki za uporabniške profile, ter v veliko primerih podatki o dejavnostih uporabnikov v aplikaciji. Zaradi obdelave vseh teh in mnogo drugih podatkov mora večina mobilnih aplikacij delovati v skladu z uredbo. Razvijalci mobilnih aplikacij morajo torej poznati zahteve za skladnost z uredbo in se držati njenih pravil.

Kot že omenjeno, uredba uvaja veliko novih zahtev, vendar pri izvajanju le-teh razvijalcem pušča precej proste roke. V diplomskem delu sem zbrala in na čim bolj razumljiv način opisala glavne določbe uredbe, ki bi jih moral poznati vsak, ki ima opravka z obdelavo osebnih podatkov. Cilj diplomske naloge je prikazati, kako razvijalec ustvari aplikacijo, ki je skladna z uredbo. S pregledom določil uredbe sem definirala kategorije aplikacij, ki bi se jih dalo določiti glede na vpliv oziroma potrebne ukrepe za skladnost z GDPR-jem. Za praktični prikaz implementacije zahtev sem razvila tudi vzorčno mobilno aplikacijo.

V drugem poglavju diplomskega dela je podanih nekaj osnovnih informacij o uredbi GDPR, katere pomembni deli vsebine so nekoliko bolj podrobno opisani v naslednjem poglavju, „Vsebina uredbe“. V četrtem poglavju omenim problem v primeru nepripravljenosti na zahteve posameznikov, podam primer zlorabe GDPR-ja s strani uporabnika in skušam določiti kategorije aplikacij glede na zahteve uredbe. V petem poglavju je predstavljena vzorčna mobilna aplikacija Smučarski skoki, za katero v naslednjem poglavju prikažem pristop k preverjanju in izpolnjevanju skladnosti mobilne aplikacije z uredbo. V podrazdelkih so najprej opisani praktični pristopi k razvoju skladne rešitve, nato pa je način izpolnjevanja zahteve opisan še na konkretnem primeru aplikacije.

Poglavje 2

Splošno o GDPR

GDPR želi prebivalcem EU omogočiti večji nadzor nad uporabo in pretokom njihovih osebnih podatkov. Poleg tega naj bi pripomogla k zvišanju ravni varstva osebnih podatkov in zagotovila usklajeno in enotno ukrepanje v primeru kršitev.

Uredba je bila sprejeta aprila 2016 s strani Evropskega parlamenta. Določeno je bilo dvoletno uvajalno obdobje, v katerem naj bi se vse članice EU pripravile na veljavo uredbe. V veljavo je stopila 25. maja 2018 in je splošno zavezujoča in veljavna v vseh državah članicah Evropske unije. Nanaša se na vse posameznike, organizacije in podjetja, ki delujejo znotraj EU, kot tudi tiste, ki se nahajajo izven Unije, vendar obdelujejo podatke o prebivalcih EU. To na primer pomeni, da mora GDPR upoštevati vsak že z objavo obrazca, v katerega uporabnik vpiše svoje kontaktne podatke in se nahaja na spletni strani, dostopni tudi prebivalcem EU. Uredba je neodvisna od tehnologije in obsega tako avtomatsko kot ročno procesiranje podatkov. Na koga potem GDPR ne vpliva? Pravila uredbe ne zajemajo posameznikov, ki osebne podatke obdelujejo iz osebnih razlogov ali v namen domače dejavnosti, ki ni povezana s poklicno ali komercialno dejavnostjo. Torej, posamezniku, ki na primer hrani lasten imenik, kateri vključuje elektronske naslove ljudi, ki jih želi povabiti na srečanje, pravil uredbe ni treba upoštevati. Druga izjema pa so osebni podatki pravnih oseb in umrlih, za katere se uredba prav tako

ne uporablja.

Z določitvijo zakonov v vseh članicah EU se je pridobila konsistentnost, ki naj bi zmanjšala probleme pri prehajanju podatkov med državami znotraj Unije. Uredba določa okvirje, oziroma neka osnovna pravila in zagotavlja, da se bodo ta pravila uveljavila in spremljala, državam članicam pa dopušča oziroma prepušča, da nekatere zakone same še bolj opredelijo, omejijo, ter jih vključijo v svoje pravo. V Sloveniji bo za to skrbel Zakon o varstvu osebnih podatkov, ZVOP-2, ki bo nadomestil Zakon o varstvu osebnih podatkov ZVOP-1, ki je veljal od leta 2004. ZVOP-2 zaenkrat še ni bil sprejet, predlog zakona pa je že v zakonodajnem postopku [11].

Poglavje 3

Vsebina uredbe

GDPR določa pravila o varstvu osebnih podatkov pri njihovi obdelavi in pravila o prostem pretoku osebnih podatkov v EU [7]. Pod obdelavo uvršča vsa dejanja v zvezi z osebnimi podatki, torej zbiranje, hranjenje, urejanje, spreminjanje, razkritje, izbris, uničenje, prenos osebnih podatkov itd. Med osebne podatke pa po uredbi spadajo vsi podatki, ki se nanašajo na določljivega posameznika. Posameznika lahko določajo ime, fizične, kulturne, genetske lastnosti, naslov bivanja, IP naslov itd.

Definicija 3.1 (Psevdonimizacija) *Psevdonimizacija je obdelava osebnih podatkov na način, da podatkov, ki so rezultat takšne obdelave, brez dodatnih informacij ni več možno pripisati posamezniku. Dodatne informacije se hranijo ločeno, s tehničnimi in organizacijskimi ukrepi pa se omeji dostop do njih.*

Definicija 3.2 (Anonimizacija) *Anonimizacija osebnih podatkov je postopek pretvorbe osebnih podatkov v „anonimizirane podatke“, ki se jih kljub dodatnim informacijam ne da pripisati posamezniku.*

Uredba anonimiziranih podatkov sicer ne vključuje, vendar je pri anonimizaciji treba biti pazljiv, saj je ni tako lahko doseči. To, da se na primer ne hrani imen in priimkov ali EMŠA, še ne pomeni, da se osebe v neki množici podatkov ne da identificirati. Primer bi bila lahko skupina športnikov, kjer

nekdo izstopa od ostalih po svoji telesni višini. V takem primeru bi telesna višina osebe omogočala določitev posameznika, in bi obdelava osebnih podatkov, ki vključujejo informacijo o telesni višini, spadala pod uredbo.

V uredbi so definirane še posebne vrste osebnih podatkov, kamor med drugimi sodijo tudi podatki o rasi, etničnem poreklu, verskem prepričanju, genetski podatki, biometrični podatki, podatki v zvezi z zdravjem ter podatki o spolni usmerjenosti. Obdelovanje teh podatkov je prepovedano, razen v primeru izrecne privolitve v obdelovanje teh podatkov s strani posameznika in ostalih izjem, ki so poleg definicije posebnih vrst osebnih podatkov navedene v 9. členu uredbe. Pri obdelavi posebnih vrst osebnih podatkov je zaradi njihove občutljivosti treba uporabljati dodatne zaščitne ukrepe.

GDPR podaja dve ključni osebi pri obdelavi osebnih podatkov, upravljalca in obdelovalca osebnih podatkov.

Definicija 3.3 (Upravljalec) *Upravljalec osebnih podatkov je tisti, ki definira katere podatke naj se obdeluje in kako; torej določa namene ter sredstva za obdelavo osebnih podatkov.*

Definicija 3.4 (Obdelovalec) *Obdelovalec obdeluje podatke na način, ki ga je podal upravljalec. Obdelovalec deluje v imenu upravljalca, njegove obveznosti pa morajo biti navede v pogodbi oziroma drugem pravnem aktu med njima. Obdelovalec brez navodil upravljalca osebnih podatkov ne sme obdelovati, razen v primeru, da je to dolžan storiti po pravu Unije ali države članice.*

Prenosi osebnih podatkov v države izven Unije in mednarodne organizacije se lahko izvedejo le v skladu s pogoji, ki jih navaja 5. poglavje uredbe. Glavni razlog za to je, da želi uredba tudi ob prenosih osebnih podatkov zagotoviti enako varnost podatkov. Komisija tako določi države, ki zagotavljajo ustrezno raven varstva osebnih podatkov. Prenos v te države je dovoljen. V kolikor država, v katero upravljalec želi prenesti osebne podatke, ni na seznamu ustreznih držav, mora upravljalec sam poskrbeti za ustrezne zaščitne ukrepe, ali pa mora veljati ena od izjem, navedenih v 49. členu uredbe.

3.1 Načela uredbe

GDPR v 2. poglavju opredeljuje 7 načel, ki morajo biti izpolnjenja pri vsaki obdelavi osebnih podatkov.

3.1.1 „Zakonitost, pravičnost in preglednost“

Osebni podatki morajo biti obdelani v skladu z zakonom, pošteno in pregledno posamezniku, katerega osebni podatki se obdelujejo. Preglednost upravljalec doseže tako, da posamezniku omogoči lahek dostop do informacij, ki jih poda na razumljiv način.

Da je obdelava osebnih podatkov zakonita, mora veljati vsaj ena od naslednjih možnosti:

- upravljalec je pridobil privolitev posameznika v obdelavo njegovih osebnih podatkov za namene, za katere bodo ti podatki obdelani,
- upravljalec ima s stranko sklenjeno pogodbo in ga k obdelovanju njenih osebnih podatkov zavezuje pogodbena obveznost,
- upravljalec je primoran obdelovati osebne podatke za izpolnitev pravnih obveznosti,
- obdelava osebnih podatkov je potrebna za zaščito posameznikovih življenjskih interesov,
- obdelava je potrebna za opravljanje naloge, ki je v javnem interesu,
- upravljalec obdeluje osebne podatke posameznikov zaradi svojih zakonitih interesov in je predhodno preveril, da temeljne pravice in svoboščine zadevnih posameznikov ne prevladajo nad njegovimi interesi.

V kolikor je pravna podlaga za obdelavo privolitev posameznika, mora biti ta jasna in nedvoumna. Posameznik se mora zavedati, v kaj bo privolil, ter v kakšnem obsegu. Sem torej ne spadajo več samodejno obkljukana potrditvena polja, ki jih mora posameznik odkljukati v primeru, da ne želi dati privoljenja v zbiranje podatkov, kjer je po možnosti navedena kopica nerazumljivih in nejasnih informacij, ki uporabnika le zmedejo in tako ne ve

več, v kaj točno bo privolil. Seveda se privolitev lahko še vedno zbere preko potrditvenega polja, vendar mora oseba to polje jasno obkljukati. Obstajati mora torej neko jasno potrditveno dejanje. Če je privolitev dana v pisni obliki in so zraven vključene tudi druge zadeve, se mora privolitev v zbiranje in obdelavo podatkov jasno ločevati od drugih zadev. Upravljalec mora biti po 7. členu uredbe vedno zmožen dokazati, da je oseba privolila v zbiranje in drugo obdelavo svojih osebnih podatkov. Preklic privolitve mora biti možno opraviti enostavno in enako hitro kot privolitev samo. O možnosti preklica mora biti posameznik obveščen še pred privolitvijo.

Otroci se običajno manj zavedajo tveganj, ki jih prinese obdelovanje njihovih osebnih podatkov, zato potrebujejo dodatno pozornost in varstvo osebnih podatkov. Obdelava osebnih podatkov otrok, mlajših od 16 let, je tako v skladu z 8. členom GDPR-ja zakonita le, če v obdelavo podatkov privolijo njihovi zakoniti zastopniki. Izjema so storitve, ki so namenjene neposredno otrokom, njihov cilj pa je varovanje otrokovih koristi. V Sloveniji bo v primeru potrditve predloga ZVOP-2 ta starostna meja 15 let [11]. Upravljalec si mora tako razumno prizadevati za preverjanje starosti posameznikov, katerih osebne podatke obdeluje, in glede ugotovitev primerno ukrepati. Tu je seveda treba upoštevati trenutno razpoložljive tehnologije. Kljub zahtevi po privolitvi v obdelavo s strani otrokovih staršev, lahko otrok sam kadarkoli zahteva uveljavitev katerekoli pravice, ki jo narekuje uredba (do vpogleda, omejitve, pozabe . . .), ne da bi za to potreboval soglasje staršev. V kolikor so ciljne stranke storitve tudi otroci, je treba dodatno poskrbeti za razumljivost vseh informacij, ki jih uporabnik dobi v okviru storitve.

3.1.2 „Omejitev namena“

Namen obdelave mora biti jasno opredeljen in zakonit. Osebnih podatkov, ki so bili zbrani v zakonit namen, se ne sme uporabiti v nov, prvotnemu nezdružljiv namen. V kolikor želi upravljalec osebne podatke obdelovati v nov namen, mora zanj imeti zakonito podlago.

3.1.3 „Najmanjši obseg podatkov“

Obdelujejo naj se le tisti podatki, ki so zares potrebni za delovanje oziroma izpolnitev namena. Na primer, za obveščanje o dogodkih v prihodnosti prek elektronske pošte ne potrebujemo tudi posameznikove telefonske številke ali informacije o njegovi najljubši barvi. Po uredbi GDPR mora vsaka organizacija za vse osebne podatke, ki jih pridobiva od posameznikov, utemeljiti, zakaj jih potrebuje, ter kako so ti podatki obdelani.

3.1.4 „Točnost“

Netočni osebni podatki morajo biti posodobljeni ali izbrisani, za kar mora poskrbeti upravljalec. Odgovoren je za sprejemanje razumnih ukrepov, ki pomagajo zagotoviti točnost podatkov.

3.1.5 „Omejitev shranjevanja“

Osebni podatki, ki omogočajo identifikacijo posameznikov, se lahko hranijo le toliko časa, kot ga zahteva namen obdelave. Tu lahko pride do odstopanj v posebnih primerih, navedenih v 5. členu uredbe, kot so statistični nameni, zgodovinsko-raziskovalni nameni obdelave, itd.

3.1.6 „Celovitost in zaupnost“

Poskrbeti je treba za zaščito podatkov, ki se jih obdeluje. To se, kot je zapisano v 24. členu uredbe, lahko zagotovi tako z ustreznimi tehničnimi kot organizacijskimi ukrepi. Osebne podatke je treba zaščititi pred zunanjimi grožnjami (npr. zlonamerni vdori) in pred notranjimi grožnjami (npr. neprimerno ravnanje zaposlenega).

3.1.7 „Odgovornost“

Upravljalec mora biti sposoben dokazati, da obdeluje podatke v skladu z vsemi prejšnjimi načeli in posledično v skladu z uredbo.

3.2 Pravice posameznikov

GDPR določa kar nekaj pravic, ki jih lahko uveljavlja posameznik, na katerega se nanašajo osebni podatki. Nekatere od teh pravic omejujejo zakonito obdelavo upravljalca, vendar jih morajo izpolnjevati vse organizacije oziroma podjetja, ki obdelujejo osebne podatke, brez izjem. Pomembno je, da se obdelovalec kljub temu, da ima uredba običajno nanj manjši vpliv, pravic posameznikov zaveda. Ob uveljavi katere od pravic mora upravljalec posamezniku v roku enega meseca, oziroma v roku treh mesecev v primeru zahtevnejših prošenj, na zahtevo zagotoviti informacije o ukrepih.

3.2.1 Pravica do preglednih informacij

Upravljalec mora posamezniku ves čas zagotavljati pregled nad obdelavo njegovih podatkov. Torej, pred začetkom zbiranja podatkov oz. ko upravljalec pridobi podatke, v primeru da jih ni pridobil od posameznika, na katerega se nanašajo, v času obdelave, ter ob posebnih dogodkih, npr. ob morebitnem vdoru ali kateri drugi kršitvi pravic posameznika. Informacije, ki jih uporabnik prejme od upravljalca, morajo biti podane v preprostem in razumljivem jeziku.

Ko upravljalec zbere osebne podatke posameznika, mu mora med drugimi sporočiti podatke o upravljalcu, ter podati informacije o tem, zakaj bo obdeloval njegove podatke, kako dolgo se bodo podatki hranili in kdo bo imel dostop do njih. Posameznik mora biti seznanjen tudi z možnostjo vpogleda v zbrane osebne podatke, možnostjo urejanja in izbrisa podatkov. Če se kasneje upravljalec odloči obstoječe podatke uporabiti v nove namene, o katerih oseba, na katero se nanašajo, še ni bila obveščena, mora o novih namenih obdelovanja in vseh ostalih informacijah, ki naj bi jih posameznik ob obdelavi njegovih osebnih podatkov prejel, upravljalec posameznika ponovno obvestiti. Seveda mora, kot že omenjeno pri načelu omejitve namena, upravljalec za nov namen imeti pravno podlago.

3.2.2 Pravica dostopa

V 15. členu uredbe [7], je podana pravica dostopa posameznika, ki mu omogoča od upravljalcev dobiti informacijo o tem, ali se pod njihovim nadzorom obdelujejo nanj navezujoči osebni podatki. Če je temu tako, mora imeti posameznik možnost dostopa in pridobitve kopije teh podatkov. V primeru elektronske zahteve morajo biti tudi povratne informacije podane v splošno uporabljeni elektronski obliki, razen če bi posameznik zahteval drugače. Poleg tega mu mora ob podani zahtevi upravljalec podati informacije o namenu obdelave, o vrsti hranjenih osebnih podatkov, o viru pridobitve podatkov v primeru, da ti niso bili pridobljeni od zadevnega posameznika, informacijo o tem, kdo vse lahko dostopa do njegovih osebnih podatkov, kako dolgo se bodo podatki hranili (kolikor natančno je to mogoče določiti), informacije o ostalih pravicah, o možnosti vložitve pritožbe, o sprejetih zaščitnih ukrepih v primeru, da se podatki prenašajo drugam, ter informacijo o tem, ali na podlagi podatkov, ki se hranijo, obstaja kakšno avtomatizirano sprejemanje odločitev. V primeru, da avtomatizirano sprejemanje odločitev obstaja, mora biti posameznik seznanjen z namenom takšne obdelave ter s posledicami, ki jih prinaša.

3.2.3 Pravica do prenosljivosti podatkov

S pravico do prenosljivosti podatkov ima vsak možnost, da tudi sam upravlja s svojimi osebnimi podatki. Posamezniku so olajšani prenos, shranjevanje, kopiranje in ponovna uporaba podatkov, ter posledično tudi zamenjava ponudnikov storitev.

V primeru, da je podlaga za zakonitost obdelave osebnih podatkov privolitev posameznika ali pa je obdelava potrebna za izvajanje pogodbe, ima oseba, ki je upravljalcu posredovala svoje podatke, pri njem pravico do pridobitve teh podatkov v, kakor je zapisano v 20. členu uredbe, „strukturirani, splošno uporabljani in strojno berljivi obliki“. Prav tako bi moral imeti posameznik možnost prenosa teh podatkov k drugemu upravljalcu brez oviranja

upravljalca, ki jih obdeluje trenutno (npr. z zaračunavanjem za izročevanje podatkov, nepotrebnim zavlačevanjem ...). Kadar je med upravljalcema direkten prenos tehnično izvedljiv, je na željo stranke upravljalec, ki trenutno hrani njene podatke, te primoran neposredno posredovati drugemu upravljalcu. Upravljalec, ki sprejema podatke od drugega, lahko sprejme le tiste podatke, ki jih potrebuje za obdelavo (upoštevanje načela najmanjšega obsega podatkov), ni pa mu jih treba sprejeti in obdelovati, v kolikor sam tega ne želi. Upravljalec, ki je na zahtevo za prenos posamezniku ali drugemu upravljalcu posredoval osebne podatke, ni odgovoren za obdelavo, ki jo kasneje izvajata posameznik ali upravljalec, ki je osebne podatke prejel. Posameznik, ki je pri upravljalcu podal zahtevo za prenos svojih osebnih podatkov, lahko po prenosu še vedno uporablja njegove storitve. Zahteva za prenos podatkov še ne pomeni, da se morajo po prenosu ti osebni podatki samodejno tudi izbrisati. V kolikor pa posameznik želi, da se njegovi osebni podatki pri upravitelju tudi izbrišejo, mora za to poskrbeti z uveljavitvijo pravice do izbrisa.

Pravica do prenosljivosti podatkov velja le za podatke, ki se obdelujejo z avtomatiziranimi sredstvi, in ne pokriva papirnatih dokumentov.

3.2.4 Pravica do popravka

V kolikor so podatki, ki jih hrani upravljalec netočni, jih mora ob obvestitvi o popravkih s strani osebe, na katero se podatki nanašajo, posodobiti. Enako velja za nepopolne podatke, katere ima posameznik pravico dopolniti. Upravljalec je dolžan osebe, ki so jim bili osebni podatki razkriti, obvestiti o popravkih.

3.2.5 Pravica do izbrisa oz. „pravica do pozabe“

Precej pomembna pravica za vsakega je „pravica do pozabe“, ki omogoča, da je upravitelj na posameznikovo zahtevo dolžan izbrisati vse osebne podatke, ki to osebo zadevajo. Posameznik lahko pravico do izbrisa uveljavi kadar

upravljalec in obdelovalec za obdelovanje podatkov nimata več upravičenega razloga. Med uveljavitve pravice do izbrisa spadajo:

- preklic soglasja o obdelavi osebnih podatkov s strani posameznika,
- nepotrebnost podatkov za namene za katere so bili zbrani in so se obdelovali,
- ugovor obdelavi s strani posameznika (kadar ima pravico do ugovora),
- nezakonita obdelava osebnih podatkov,
- potreba po izbrisu za izpolnitev pravnih obveznosti.

Organizacijam ob zahtevi izbrisa osebnih podatkov po 3. točki 17. člena uredbe tega ni treba storiti v primeru, da so obdelovani osebni podatki potrebni za uresničevanje pravice do svobode izražanja, kadar njihovo hrambo narekuje pravna obveznost ali pa iz razlogov javnega interesa. To so na primer interesi glede javnega zdravja, kot tudi znanstveno-raziskovalnih nameni, med katere spada tudi tehnološki razvoj. V kolikor bi zahtevani izbris podatkov predstavljal resno oviro, oziroma bi onemogočal obdelavo v namen raziskave, zadevnih podatkov ni treba izbrisati. Pogoj za to, omenjen v istem členu uredbe, je, da se izvajajo ustrezni zaščitni ukrepi, predvsem minimizacija obsega podatkov.

3.2.6 Pravica do omejitve obdelave

V primeru, da upravljalec osebnih podatkov posameznika ne potrebuje več za namene obdelave, vendar jih posameznik še vedno potrebuje za uveljavljanje ali izvajanje pravnih zahtevkov, lahko posameznik doseže, da upravljalec obdelavo omeji. Drugi razlogi za omejitev obdelave so lahko še oporekanje točnosti podatkov, nezakonita obdelava osebnih podatkov, kjer posameznik, na katerega se nanašajo, ne želi izbrisa, vendar le omejitev obdelave, vložitev ugovora obdelavi. Omejitev obdelovanja pomeni, da se osebni podatki posameznika lahko le hranijo [12]. Za druge vrste obdelave, pa upravljalec

potrebuje posameznikovo privolitev[1].

3.2.7 Pravica do ugovora

V kolikor je obdelava zakonita na podlagi obdelovanja osebnih podatkov zaradi upravljavčevih zakonitih interesov ali pa je obdelava potrebna za izvajanje nalog, ki so v javnem interesu, lahko posameznik ugovarja obdelavi zaradi posebnih razlogov, ki vplivajo nanj. Kadar pa se posameznikovi osebni podatki obdelujejo za namene neposrednega trženja, ima pravico do ugovora kadarkoli.

3.2.8 Pravica glede avtomatiziranega sprejemanja odločitev (vključno z oblikovanjem profilov)

Avtomatizirano sprejemanje odločitev in profiliranje se uporabljata na vedno več področjih, saj je z današnjo tehnologijo vedno lažje analizirati in predvidevati človekove značilnosti. Ker pa se to izkorišča in uporablja brez vedenja oseb, ki jih odločitve zadevajo, so v uredbi GDPR posameznikom pravice zagotovili tudi na tem področju.

Avtomatizirano sprejemanje odločitev, ki vključuje profiliranje, tako v splošnem ni dovoljeno, obstajajo pa primeri, ki to dovoljujejo:

1. Oseba, na katero se nanašajo podatki, je podala izrecno privolitev v takšno obdelavo.
   Pri profiliranju se velikokrat ne uporabljajo le podatki, ki so bili pridobljeni neposredno od osebe, na katero se nanašajo, vendar tudi takšni, ki so bili izpeljani iz drugih podatkov. Zato morajo upravljalci v primeru takšnih privolitev posameznike natančno seznaniti s tem, kaj vse takšno obdelovanje obsega in na kakšen način se sprejemajo odločitve.

[1]Izjeme so še uveljavljanje, izvajanje in obramba pravnih zahtevkov, varstvo pravic druge fizične ali pravne osebe, ter pomembni javni interes Unije ali države. (Splošna uredba o varstvu podatkov, člen 18(2))

2. Takšne odločitve so potrebne za sklenitev ali izvajanje pogodbe.
   Sem spadajo primeri, kjer so avtomatizirane odločitve potrebne za izvajanje storitve in privolitev ni primerna zakonita podlaga za takšno obdelavo.
3. Dovoljuje jih pravo EU ali države članice.

V primerih, ki so izjeme prepovedi uporabe avtomatiziranega sprejemanja odločitev in profiliranja, je še vedno treba poskrbeti za varnostne ukrepe, ki varujejo pravice posameznika.

3.3 Obdelava in varnost podatkov

Kot že omenjeno mora biti vsako podjetje oziroma organizacija po načelu odgovornosti sposobna dokazati, da deluje v skladu z uredbo. Pri tem jim uredba pomaga s predlogi uporabe določenih orodij. Eno izmed njih so kodeksi ravnanja, ki naj bi prispevali k pravilni uporabi uredbe. V skladu s 40. členom uredbe združenja lahko pripravijo kodekse, oziroma že obstoječe dopolnijo ali spremenijo. Ko so kodeksi odobreni s strani nadzornega organa, ali v nekaterih primerih Komisije, so ti registrirani in objavljeni.

Nadzorni organ je neodvisni organ, ki mora biti po 51. členu uredbe določen v vsaki državi članici (vsaka članica lahko določi več nadzornih organov). Odgovoren je za spremljanje skladnosti uporabe osebnih podatkov z uredbo, obravnavo pritožb in kršenja uredbe, ozaveščanje javnosti o tveganjih, pravicah in pravilih, ki jih določa uredba, sodelovanje z drugimi nadzornimi organi ... V Sloveniji ima vlogo nadzornega organa Informacijski pooblaščenec [11]. Nalogo zagotavljanja dosledne uporabe Splošne uredbe o varstvu podatkov mora izvajati tudi Evropski odbor za varstvo podatkov. Odbor je organ Unije, ki ga sestavljajo predstavniki vodilnih nadzornih organov vseh držav članic.

Za dokazovanje skladnosti z uredbo morajo podjetja z več kot 250 zaposlenimi hraniti in redno posodabljati evidenco dejavnosti obdelave. Sem spadajo vse obdelave osebnih podatkov, ki jih podjetje oziroma organizacija

izvaja, na primer zbiranje, hranjenje, posredovanje, izbris osebnih podatkov itd. Voditi jih morata tako upravljalec kot obdelovalec, ki sta nadzornemu organu na njegovo zahtevo primorana omogočiti vpogled v evidence dejavnosti obdelave. Evidence upravljalca morajo med drugimi vsebovati informacije o tem, katere osebne podatke hrani, s kakšnim namenom in kako dolgo se bodo hranili (v kolikor je mogoče podati roke za izbris določenih vrst podatkov), evidence obdelovalca pa vrste obdelave, ki jih opravlja v imenu upravljalca, opis tehničnih in organizacijskih varnostnih ukrepov, itd. Podjetja oziroma organizacije z manj kot 250 zaposlenimi morajo po določilih 30. člena uredbe hraniti le evidence tistih dejavnosti, ki se izvajajo redno, predstavljajo tveganje za pravice in svoboščine zadevnih posameznikov, ali se nanašajo na osebne podatke posebnih vrst ali kazenske evidence.

Upravljalec in obdelovalec morata ves čas zagotavljati ustrezno varnost zbranih osebnih podatkov. To lahko zagotovita z vrsto varnostnih ukrepov, tako tehničnih kot organizacijskih. Ker je v svetu vedno več novih napadov na podatke organizacij, je treba ves čas skrbeti za varnostne protokole, da le-ti ne dobijo varnostnih lukenj, ki bi se jih dalo izkoristiti. Izvajati je torej treba redno ocenjevanje, vrednotenje in testiranje varnosti. Za zagotavljanje varnosti osebnih podatkov je potrebnega precej razmisleka glede možnih fizičnih in tehničnih incidentov, saj je ob takem dogodku treba zagotoviti čimprejšnji ponovni dostop do podatkov. Pomembna je ocena tveganja obdelave in njenega obsega zaradi možnosti nepooblaščenega dostopa do podatkov, razkritja, izgube ali uničenja podatkov itd. Uredba spodbuja izvajanje varnostnih ukrepov predvsem glede na stopnjo teh tveganj, zato imajo tista podjetja, ki obdelujejo večje količine osebnih podatkov, tudi nekoliko večje obveznosti.

Kadar upravljalec in obdelovalec veliko upravljata s posebno vrsto podatkov (na primer bolnišnice, socialno-varstveni zavodi, itd.), mora biti imenovana pooblaščena oseba za varstvo podatkov. Njena naloga sta predvsem svetovanje in nadzor na področju varstva osebnih podatkov. Prav tako lahko stopijo v kontakt z njo posamezniki v primeru vprašanj glede obdelave nji-

hovih osebnih podatkov. Pooblaščena oseba za varstvo podatkov mora za opravljanje vloge imeti dovolj strokovnega znanja na področju varstva podatkov. Vključena in seznanjena mora biti z vsem, kar zadeva varnost podatkov, za opravljanje svojega dela pa mora imeti zagotovljen zadosten dostop, za kar sta odgovorna upravljalec in obdelovalec. Pooblaščeno osebo za varstvo podatkov morajo določiti tudi javni organi in telesa, ter podjetja, ki morajo za svoje poslovanje posameznike redno in sistematično spremljati. To so na primer banke, zaposlovalne agencije, podjetja, ki ponujajo informacijske sisteme za upravljanje osebnih podatkov itd. Po določitvi pooblaščene osebe se morajo kontaktni podatki le-te sporočiti nadzornemu organu, saj je ta tista, ki sodeluje z nadzornim organom in jim predstavlja kontaktno točko organizacije oziroma podjetja.

Kadar pri določeni vrsti procesiranja lahko pride do velikih tveganj glede pravic in svoboščine oseb, je pred obdelavo obvezno izvesti ocene učinka v zvezi z varstvom podatkov. Tudi te so upravljalcu v pomoč pri zagotavljanju načela odgovornosti. Namen izvedbe ocene je opisati potek in potrebnost obdelave, vnaprejšnje prepoznavanje tveganj in določitev ukrepov za njihovo obvladovanje ter ocena sorazmernosti obdelave glede na njen namen. Za oceno je torej potrebno ugotoviti, kakšne so verjetnosti in učinki tveganj. To je predvsem pomembno pri uvedbi novih tehnologij za obdelavo osebnih podatkov ali pa pri vrednotenju, točkovanju oseb, avtomatiziranem obdelovanju (vključno z ustvarjanjem profilov), obdelavi občutljivih podatkov, obdelavi podatkov v velikem obsegu itd. Ker je ocena učinka za upravljalca uporabna, jo je dobro izvesti tudi v primerih, kjer ni povsem jasno, ali je potrebna. Upravljalcem je lahko v pomoč pri odločitvi o izvedbi ocene seznam vrst dejanj obdelave, ki oceno zahtevajo. Ta seznam in pa neobvezni seznam, ki vsebuje vrste obdelave, za katere ocena učinka ni potrebna, mora v skladu s 35. členom uredbe določiti in objaviti nadzorni organ. Ob izvedbi ocene je treba za mnenje prositi pooblaščeno osebo za varovanje podatkov (v kolikor ta obstaja). V primeru, da upravljalec ne najde ustreznih ukrepov za zmanjšanje tveganja na sprejemljivo raven, mora za mnenje prositi

tudi nadzorni organ. Pomembno je, da se ocena učinka izvaja redno in ni le enkratni dogodek, saj vse spremembe lahko vplivajo nanjo. V primeru sprememb tveganj obdelave, pa je potrebno preveriti tudi, ali obdelava, kakršna se uporablja trenutno, deluje v skladu z oceno učinka.

3.3.1 Kršitve varstva osebnih podatkov

V primeru kršitev varstva osebnih podatkov, definiranih v 4. členu uredbe, kjer bi bile lahko ogrožene posameznikove pravice in svoboščine, mora upravljalec o kršitvi takoj obvestiti nadzorni organ. Kršitev varstva osebnih podatkov je po uredbi varnostni incident, v katerem je prišlo do nenamerne ali nezakonite spremembe, izgube, uničenja ali pa nepooblaščenega dostopa oziroma razkritja osebnih podatkov. To so lahko na primer posredovanje osebnih podatkov napačni osebi, kraja računalniške opreme z osebnimi podatki, dostop in uničenje podatkovnih baz, ki vsebujejo osebne podatke s strani nepooblaščenih oseb ... Nadzorni organ mora biti o kršitvi obveščen najkasneje v roku 72 ur po zaznanju kršitve. Obvestilo kršitve mora med drugimi vsebovati obseg in kategorijo kršitve, kontaktne informacije osebe, ki je pooblaščena za varstvo podatkov (za pridobitev več informacij), opis posledic kršitve ter opis ukrepov, ki jih bo upravljalec izvedel oziroma jih predlaga.

Če predstavlja kršitev veliko tveganje za posameznika, katerega podatki so bili vključeni oziroma razkriti pri kršitvi, je o tem treba obvestiti tudi samega posameznika. Ne glede na to, ali kršitev predstavlja tveganje za posameznika ali ne, pa mora upravljalec vsako kršitev dokumentirati. V dokumentacijo morajo biti vključeni podatki o dejstvih, ki zadevajo kršitev, njenih učinkih ter ukrepi, ki so bili sprejeti.

3.4 Kazni v primeru kršitev uredbe

Vsak posameznik, ki meni, da je pri obdelavi njegovih osebnih podatkov prišlo do kršenja, lahko pri nadzornemu organu vloži pritožbo. Nadzorni or-

gan je odgovoren to pritožbo sprejeti in obravnavati, ter vlagatelja pritožbe o njenem stanju in odločitvi o pritožbi obvestiti. Posameznik, ki je kot posledico kršenja uredbe utrpel škodo (tako premoženjsko kot nepremoženjsko), ima pravico, da od obdelovalca ali upravljalca dobi odškodnino, saj je le ta odgovoren za vso nastalo škodo pri obdelavi.

Kazni se ovrednotijo glede na okoliščine kršitve. Upošteva se dejstvo, ali je bila kršitev namerna ali je prišlo do nje zaradi malomarnosti, kako obsežna je bila kršitev (število prizadetih posameznikov ter v kakšnem obsegu jih je kršitev prizadela), trajanje kršitve, ukrepi, ki so bili sprejeti da bi se posledice kršitve za posameznika olajšale, predhodne kršitve upravljalca in obdelovalca, vrsta osebnih podatkov, ki so bili izpostavljeni pri kršitvi, sodelovanje organizacije, ter druge olajševalne ali oteževalne okoliščine, ki igrajo vlogo v posameznem primeru.

Možne kazni so opomin, prepoved obdelave, ki je lahko le začasna ali pa celo dokončna, in globa, ki lahko znaša tudi do 20 milijonov evrov ali 4 % skupnega svetovnega letnega prometa podjetja (kar predstavlja višji znesek). V vsakem primeru pa naj bi bila kazen učinkovita, sorazmerna in odvračilna.

Poglavje 4

Obvladovanje zahtev

4.1 Zahteve s strani uporabnikov

Kazni so torej visoke, zahtev, ki jih ima posameznik pravico podati, pa ni malo. V kolikor bi se nekdo odločil od upravljalca pridobiti vse informacije, do katerih ima pravico, bi mu lahko naložil kar precej dela. S strani uporabnikov bi tako lahko hitro prišlo do zlorabe GDPR. Takšen primer bi bil „The nightmare letter“ [16], kjer je avtor v spletni objavi podal primer obsežne zahteve uporabnika za dostop do osebnih podatkov v skladu s 15. členom uredbe. V njej najprej prosi za informacijo o tem, ali se obdelujejo njegovi osebni podatki. V kolikor se obdelujejo, želi izvedeti, katere kategorije osebnih podatkov so vključene v obdelavo. Za vsako kategorijo hranjenih osebnih podatkov zahteva tudi informacije o roku hrambe. Poleg tega prosi za vpogled v vse svoje osebne podatke, ki jih ima upravljalec, kopijo le-teh, ter podatke o tem, v katerih državah so njegovi podatki shranjeni ali dostopni. Nato prosi za podroben opis vseh namenov obdelave, seznam vseh tretjih ponudnikov storitev, ki so jim bili razkriti njegovi osebni podatki in navedbo varnostnih ukrepov, ki so bili vzpostavljeni v zvezi z naštetimi ponudniki. Če upravljalec podatkov, ki se jih obdeluje, ni pridobil od uporabnika, želi dobiti vse informacije o viru osebnih podatkov. V primeru uporabe avtomatiziranega odločanja, prosi še za podatke o pravni podlagi in informacije o

možnih posledicah takšne obdelave. V nadaljevanju uporabnika zanima, do katerih kršitev varstva podatkov je prišlo, komu vse so bili razkriti njegovi osebni podatki ob takšnih dogodkih, kdaj je prišlo do kršitve itd. Vedeti želi tudi precej podrobnosti o tem, katerih varnostnih ukrepov se drži upravljalec. Na primer, ali se uporabljajo sistemi za zaznavo vdorov, šifriranje, avtentikacija, avtorizacija, orodja za revizijske sledi itd. Na koncu pa prosi še za nekaj informacij v zvezi z njegovimi zaposlenimi, kot so na primer podatki o varnostnih postopkih za zagotavljanje, da zaposleni z dostopom do njegovih osebnih podatkov, teh ne razkrivajo drugim.

V kolikor upravljalec nima vseh teh informacij nekje dokumentiranih in sistema pripravljenega tako, da posamezniku lahko te podatke hitro zagotovi, zna z zahtevami uporabnikov imeti ogromno dela, kar bi lahko povzročilo težko shajanje z roki za odziv na zahteve, ki so navedeni v poglavju o pravicah posameznika. Kot sem že omenila, so takšne zahteve zloraba GDPR, saj bi se skupina ljudi s takšnimi zahtevami lahko spravila nad upravljalca, ki bi v takem primeru moral večino časa nameniti izpolnjevanju zahtev, ne pa svoji primarni dejavnosti.

4.2 Kategorije aplikacij glede na zahteve uredbe

Ker uredba ne postavlja vsem enakih pravil in določa precej izjem, oziroma v nekaterih primerih uvaja dodatne dolžnosti, lahko določimo nekaj kategorij in podkategorij aplikacij glede na zahteve uredbe, ki jih je treba upoštevati. Ločiti se da dve glavni kategoriji:

- Aplikacije, ki jih GDPR ne zadeva

  Zahtevam uredbe se najlažje izognejo tisti, ki ne obdelujejo osebnih podatkov. Takih aplikacij je precej malo, saj večina aplikacij z obdelavo osebnih podatkov, če ne drugega, izboljša uporabniško izkušnjo. Uredba ne velja tudi za tiste, ki obdelujejo osebne podatke, vendar ne delujejo v Uniji, njihove aplikacije pa niso namenjene prebivalcem Unije, zato naj ne bi obdelovale njihovih osebnih podatkov. To, da

upravljalec in obdelovalec nudita storitve prebivalcem Unije, mora biti jasno razvidno in se pri ugotovitvi ne upošteva le dostopnost storitve. V primeru spletne trgovine bi o tem, komu je storitev namenjena, lahko povedala jezik, ki se lahko uporablja v tej aplikaciji, ali pa valuta, s katero se lahko plačuje. V to kategorijo sodi še obdelava anonimiziranih podatkov, podatkov umrlih ali pravnih oseb, ter obdelava v okviru domače dejavnosti.

- Aplikacije, ki jih GDPR zadeva

  Ta kategorija je precej obsežna, zato jo razdelimo na več podkategorij. Vsem podkategorijam je skupna zahteva po upoštevanju načel obdelave, ter zagotavljanje pravic posameznikov in varnosti hranjenih podatkov. Podkategorije so definirane z naslednjimi lastnostmi obdelave:

  1. Upravljalec za obdelavo potrebuje privolitev posameznika

     Tej kategoriji poleg aplikacij, ki privolitev potrebujejo za zakonito podlago, pripadajo še tiste, ki obdelujejo osebne podatke posebnih vrst, v kolikor za obdelavo teh podatkov ne velja nobena druga izjema. Enako velja za avtomatizirano sprejemanje odločitev, vključno z oblikovanjem profilov.

  2. Osebni podatki se prenašajo v tretje države ali mednarodne organizacije

     V tem primeru mora upravljalec poskrbeti, da bo prenos potekal v skladu z uredbo in bo ustrezna raven varstva osebnih podatkov med prenosom ter pri prejemniku zagotovljena.

  3. Podjetje oziroma organizacija ima več kot 250 zaposlenih ali obdelava osebnih podatkov ni občasna

     Za aplikacije, ki sodijo v to kategorijo, morata upravljalec in obdelovalec voditi evidenco dejavnosti obdelave. Uredba tukaj daje nekaj olajševalnih okoliščin manjšim podjetjem in organizacijam, ki morajo voditi evidenco le za nekatere vrste obdelav, naštete v poglavju o vsebini uredbe.

4. Osebne podatke obdeluje javni organ ali telo

   Z izjemo delovanja v imenu sodnega organa, morajo vsi javni organi in telesa v skladu s 37. členom uredbe imenovati pooblaščeno osebo za varstvo podatkov.

5. Obdelava lahko povzroči veliko tveganje

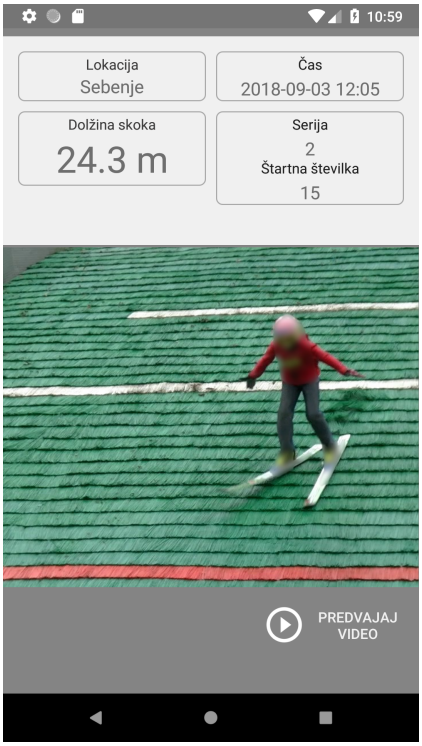
   V primeru možnosti velikih tveganj uredba vsem, tudi podjetjem z manj kot 250 zaposlenih, narekuje vodenje evidence dejavnosti obdelave. Poleg tega je ob kršitvah varstva osebnih podatkov, za obdelavo katerih so ocenjena velika tveganja, upravljalec primoran posameznika o tem tudi obvestiti. Tu lahko pride še do dodatnih obveznosti v primeru obsežne obdelave posebnih vrst osebnih podatkov ali obsežnega in sistematičnega spremljanja posameznikov. V takem primeru mora upravljalec izvajati tudi oceno učinka ter imenovati pooblaščeno osebo za varstvo osebnih podatkov.

Poglavje 5

Vzorčna mobilna aplikacija „Smučarski skoki“

Kot primer mobilne aplikacije, skladne s Splošno uredbo o varstvu podatkov, služi Android aplikacija „Smučarski skoki“, ki sem jo razvila v okviru diplomske naloge. Ta uporablja osebne podatke skakalcev in njenih uporabnikov. Glavni namen aplikacije je prikaz doskokov smučarskih skakalcev neke določene tekme.

Ob zagonu aplikacije se uporabniku najprej prikaže zaslon s seznamom tekem, katerih skoki so trenutno shranjeni. Neprijavljenim uporabnikom se pred zaslonom s tekmami prikaže še zaslon za prijavo. Ko uporabnik izbere tekmo, katere skoki ga zanimajo, se mu prikažejo slike in nekateri podatki o skokih. Prikazani podatki so odvisni od tega, kaj je bilo poslano na strežnik, in je posledično shranjeno v podatkovni bazi. V kolikor so na strežniku prisotni vsi možni podatki, dobi uporabnik poleg slike doskoka še informacije o dolžini skoka, štartni številki tekmovalca, seriji tekme, lokaciji tekme ter video posnetek doskoka, kakor je prikazano na sliki 5.1.



Slika 5.1: Posnetek zaslona - prikaz skoka.

5.1 Uporabljene tehnologije in delovanje aplikacije

Kot že omenjeno je bila aplikacija ustvarjena za mobilni operacijski sistem Android. Programska platforma Android temelji na Linuxovem jedru in je uporabljena na velikem številu raznih pametnih naprav [2]. Med razvijalci mobilnih aplikacij je priljubljena predvsem zato, ker je odprtokodna in dobro podprta. Android aplikacije so napisane v objektno usmerjenem programskem jeziku Java [14], za oblikovanje uporabniškega vmesnika pa se uporablja označevalni jezik XML [26]. Aplikacijo sem razvila v uradnem Androidovem integriranem razvojnem okolju (angl. *IDE – Integrated Development Environment*) Android Studio. Ta vključuje tudi emulator, ki simulira naprave Android. Prednost emulatorja je, da z njim razvijalec lahko testira delovanje

na različnih napravah in ravneh Androidovega API-ja.

Vsi podatki, s katerimi deluje aplikacija, so shranjeni v podatkovni bazi na strežniku. Na obeh straneh, na strani mobilne aplikacije in na strežniški strani, je sprogramiran aplikacijski vmesnik REST (REST API) [18], ki omogoča prenos podatkov na mobilni telefon in obratno. REST je arhitekturni stil, pogosto uporabljen za načrtovanje API-jev spletnih storitev. Klient za pridobivanje ali spreminjanje podatkov na strežnik pošlje zahtevo, ta pa mu vrne odgovor. Komunikacija poteka prek HTTP povezave. Za varnost podatkov se v našem primeru uporablja še šifriranje podatkov, torej HTTPS protokol. S tipom HTTP zahtevka (GET, PUT, POST, DELETE...) povemo, kateri tip operacije želimo izvesti, s potjo v naslovu URL, na katerega pošljemo zahtevo, pa povemo, katere podatke želimo pridobiti oziroma spremeniti. V naslovih je za lažje razumevanje dobro uporabljati samostalnike v množini [3]. V našem primeru tako na primer na naslovu, ki se konča z */jumpers*, v odgovoru zahteve GET dobimo podatke o vseh skakalcih. Če na koncu naslova dodamo še ID skakalca (dobimo torej obliko */jumpers/*{*jumper_id*}), se bodo ob zahtevkih, poslanih na ta naslov, izvajale operacije na podatkih posameznega skakalca, določenega z ID-jem v naslovu.

Aplikacija vse podatke, razen slik in video posnetkov, prejme v JSON obliki, jih obdela in prikaže na ekranu uporabnika. Enako velja tudi za obliko podatkov, poslanih na strežnik. JSON je format za izmenjavo podatkov, ki ga računalniki zelo enostavno generirajo in razčlenijo [15]. Sestavljen je iz dveh osnovnih oblik. Prva je zbirka parov imen in pripadajočih vrednosti, druga pa urejen seznam z vejico ločenih vrednosti v oglatih oklepajih. Na strani aplikacije se za izvajanje večine API klicev uporablja knjižnica Retrofit [24]. Retrofit je HTTP odjemalec in omogoča izvajanje tako sinhronih, kot asinhronih klicev. Poleg tega podpira tudi nekaj pretvornikov, ki podatke, pridobljene v JSON obliki, pretvorijo v javanske objekte. V aplikaciji se ob skoraj vsaki menjavi pogleda izvede eden ali več asinhronih klicev, ki na strežnik pošljejo zahtevek za pridobitev podatkov. Ob uspešnem klicu se gradnikom uporabniškega vmesnika za prikaz besedila (to so večinoma

gradniki imenovani TextView) nastavijo podatki, pridobljeni od strežnika. Za pridobitev podatkov za gradnike za prikaz slik ImageView in gradnike za prikaz video posnetkov VideoView, pa se izvedejo ločeni asinhroni klici. V primeru neuspešnih klicev, se ti zabeležijo v dnevniške datoteke, uporabnik pa na ekranu dobi obvestilo o neuspešnem klicu.

Strežniški REST API se uporablja tudi za shranjevanje podatkov o skokih, pridobljenih od zunanjega sistema. V našem primeru smo storitev integrirali v video merilno aplikacijo, ki meri dolžine smučarskih skokov. Ta odmerjeno dolžino in ostale podatke skoka v enem zahtevku pošlje na strežnik.

Na strežniku imamo torej dve glavni komponenti, API in podatkovno bazo. Vsaka komponenta teče ločeno v svojem Docker vsebniku [5]. Za podatkovno bazo smo uporabili PostgreSQL [22], odprtokoden sistem za upravljanje objektno-relacijskih baz. Ta podpira velik del standarda SQL jezika, hkrati pa ga tudi razširja. API je sprogramiran v programskem jeziku Python [23]. Python je objektno orientiran skriptni jezik. Njegova sintaksa je enostavna in lepo berljiva. Ima veliko standardno knjižnico, ki podpira mnogo pogosto uporabljenih funkcionalnosti, obstaja pa tudi veliko že napisanih modulov, ki se jih da vključiti, kar pohitri programiranje. Medtem ko je programiranje v Pythonu hitro, pa je njegovo izvajanje v primerjavi z nekaterimi drugimi jeziki, kot je na primer Java ali pa celo C, precej bolj počasno. Za vsako kombinacijo različnih naslovov URL in tipov HTTP zahtevka je implementirana ena funkcija, ki sprejme podatke zahtevka in vrne odgovor. Vmes program dostopa tudi do podatkovne baze, kjer izvaja zahtevi primerne operacije CRUD, torej operacije dodajanja, branja, spreminjanja in brisanja.

Poleg že omenjenega prikaza doskokov določenih tekem, ki predstavlja glavno funkcionalnost aplikacije, pa so preko glavnega menija dostopni še drugi pogledi, ki jih je bilo treba ustvariti, če ne drugega, zaradi skladnosti aplikacije z GDPR-jem. Uporabnik tako lahko dostopa do pogleda, kjer ima prikazane vse svoje podatke, ki se hranijo v podatkovni bazi. Tu ima še možnost urejanja teh podatkov ali pa celo izbrisa svojega uporabniškega

računa. V aplikaciji lahko uporabnik hitro najde tudi vse informacije, ki naj bi mu jih zagotovil upravljalec. Za osebo, ki bo imela vlogo administratorja aplikacije, sta ustvarjena še pogled s seznamom vseh uporabnikov aplikacije in pogled s seznamom vseh skakalcev, katerih podatki se zbirajo. Z izbiro skakalca ali uporabnika se mu odpre pogled z vsemi podatki izbranega posameznika. Poleg tega pa ima administrator v aplikaciji tudi možnost dodajanja in odstranitve skakalcev in posameznih skokov.

Poglavje 6

Skladnost aplikacije s Splošno uredbo o varstvu podatkov

Ko pride do skladnosti s Splošno uredbo o varstvu podatkov, se mora vsak razvijalec aplikacije najprej vprašati, ali obdeluje osebne podatke posameznikov. Tu se mora zavedati, da so osebni podatki po uredbi definirani zelo široko, in sem poleg imena, elektronskega naslova in ostalih precej očitnih osebnih podatkov, spadajo tudi nekateri podatki o napravi, kot sta na primer enolični identifikator naprave ali njena lokacija. Kot že omenjeno v poglavju o vsebini uredbe, so osebni podatki vsi podatki, ki določajo posameznika. Ko razvijalec aplikacije enkrat zbere in začne z obdelavo osebnih podatkov uporabnikov aplikacije, njegova aplikacija v večini primerov pade v kategorijo aplikacij, ki jih GDPR zadeva, zato mora upoštevati zahteve uredbe.

Upravljalec, kot ga definira uredba, je v primeru mobilnih aplikacij običajno ponudnik aplikacije [19]. Ta ima glavno vlogo pri skrbi za skladnost z uredbo. V kolikor aplikacija uporablja storitve tretjega ponudnika, na primer za oglaševanje, možnosti plačevanja v aplikaciji, za razne analize podatkov itd., so ti ponudniki prav tako upravljalci. Naloga glavnega upravljalca, v takem primeru ponudnika aplikacije, je, da preveri, da se storitve tretjih ponudnikov, ki jih koristi, izvajajo skladno z uredbo. V večini primerov je ponudnik aplikacije tudi obdelovalec, ni pa nujno. Za primer lahko vzamemo

podjetje, ki želi trgu ponuditi lastno aplikacijo, vendar nima znanja, da bi jo razvilo samo, zato za razvoj in vzdrževanje aplikacije najame zunanjega izvajalca. Vlogo obdelovalca ima v tem primeru zunanji izvajalec, ki deluje po navodilih ponudnika aplikacije.

6.1 Zakonitost

V kolikor je upravljalec ugotovil, da ga uredba zadeva, mora najprej poskrbeti, da bo obdelava podatkov zakonita. Upravljalci mobilnih aplikacij običajno obdelujejo podatke zakonito na podlagi privolitev, ker je obdelava potrebna za izvajanje ponujene storitve (pogodbena obveznost) ali ker je obdelava obvezna za izpolnjevanje pravnih obveznosti.

Pravna podlaga za obdelavo podatkov skakalcev so privolitve posameznikov. Za pridobitev privolitve v obdelavo s strani skakalcev je odgovoren administrator aplikacije. Prek aplikacije ta nato v bazo vnese podatke skakalca, ki je dal privolitev. V podatkovni bazi se hranijo ime, priimek in klub skakalca. Prav tako se hrani čas vnosa skakalca v podatkovno bazo, zato da vsak skakalec lahko tudi prek aplikacije dobi informacijo o tem, od kdaj se obdelujejo njegovi osebni podatki. Razlog, da skakalec svoje privolitve ne poda sam prek aplikacije, je, da le-ta kljub temu, da se mogoče strinja z obdelavo svojih podatkov, ni nujno tudi njen uporabnik. Ker je administrator tisti, ki zbira privolitve skakalcev v obdelavo, je sam odgovoren tudi za zmožnost dokazovanja teh privolitev. Veliko skakalcev je mlajših od 15 let, zato je zanje potrebno pridobiti privolitev njihovih zakonitih zastopnikov. Meja za privolitev s strani staršev oziroma skrbnikov, bi zaenkrat po uredbi lahko bila še 16 let, vendar naj bi ZVOP-2 v Sloveniji to mejo prestavil na 15 let, zato je nižjo mejo dobro upoštevati že sedaj in se tako izogniti ponovnem zbiranju privolitev.

V večini primerov aplikacij, kjer se zbirajo le podatki o njihovih uporabnikih, pa se privolitev običajno zbere neposredno od posameznika, v aplikaciji sami. Kot že omenjeno v poglavju o načelih obdelave, mora za privolitev ob-

stajati jasno potrditveno dejanje. To je najlažje implementirati prek obrazca, ki ga mora uporabnik izpolniti pred uporabo aplikacije. Posameznik se mora strinjati z vsemi nameni obdelave, zato je to najbolje narediti tako, da se v bazi za vsak namen ustvari svoj stolpec, ki predstavlja eno potrditveno polje na obrazcu. Namen obdelave je treba precej natančno definirati. Navesti, da je obdelava na primer potrebna za zagotavljanje storitev in razvoj novih funkcij še ni dovolj [19]. Za dokaz o privolitvi v obdelavo pa ne zadostuje nanašati se na pravilne nastavitve aplikacije. Uredba sama ne definira, kaj točno je potrebno za skladnost s to zahtevo, zato se tu pristopi lahko precej ločujejo. Ena možnost bi bila shranjevanje podatkov o seji, v katerih je bila izvedena privolitev, ter kopija informacij, ki jih je takrat dobil posameznik [21].

Poleg podatkov o skakalcih se v našem primeru hranijo tudi podatki o uporabnikih aplikacije. Uporabnik mora ob registraciji podati svoje ime, priimek in elektronski naslov. Ob registraciji na podan elektronski naslov nato dobi elektronsko sporočilo s potrditveno povezavo. Navedeni podatki o uporabnikih so potrebni za izvajanje storitve, zato je v našem primeru primerna zakonita podlaga pogodbena obveznost in ne privolitev posameznika. V kolikor pa bi upravljalec kasneje na zbrani elektronski naslov želel uporabnikom pošiljati še novice, bi v ta namen moral zbrati privolitev.

6.2 Varnost podatkov

Vsak razvijalec mobilne aplikacije mora že od začetka razvijanja aplikacije misliti na zasebnost uporabnikov. Ta naj bi se implementirala skozi celotni razvoj aplikacije. Vgrajeno varstvo podatkov oziroma vgrajena zasebnost (angl. *privacy by design*) ni nov koncept, je pa sedaj ena od zahtev uredbe. Poleg tega mora razvijalec poskrbeti tudi za privzeto zasebnost osebnih podatkov (angl. *privacy by default*). Kaj to pomeni? Recimo, da imamo neko družbeno omrežje, kjer uporabnik deli svoje osebne podatke z drugimi. Takšna aplikacija običajno vsebuje meni z nastavitvami zasebnosti, kjer upo-

rabnik določi, kdo vse lahko vidi njegove podatke ter katere. Vgrajena zasebnost osebnih podatkov je v tem primeru dosežena z začetno nastavitvijo, ki predstavlja maksimalno zasebnost. To nastavitev lahko uporabnik kasneje seveda po želji spremeni.

Pri vgrajeni zasebnosti nas uredba usmerja z načeloma omejitve namena in najmanjšega obsega podatkov. Ko definiramo namen našega zbiranja in nadaljnje obdelave osebnih podatkov, lahko določimo kategorije podatkov, ki so za to potrebne. Tu se mora vsak razvijalec zavedati, da manj podatkov, kot jih zbira, manj podatkov je lahko razkritih ob raznih incidentih, ki ogrožajo zasebnost uporabnikov. GDPR ne definira, katere varnostne ukrepe točno bi moral upoštevati upravljalec, vendar zahteva, da se zagotovi neka primerna stopnja varnosti glede na tveganja obdelave. Za zaščito samih podatkov na več mestih kot primera omenja šifriranje in psevdonimizacijo. Poleg teh dveh zna v nekaterih primerih priti prav tudi anonimizacija. Najpogosteje uporabljena in najvarnejša tehnika izmed njih je seveda šifriranje, saj zašifrirani podatki tistemu, ki ne pozna ključa za odšifriranje, ne dajejo nobene informacije o prvotnih podatkih. To seveda velja ob predpostavki, da so za šifriranje uporabljeni semantično varni kriptosistemi, ki pred napadalcem s polinomsko omejenimi računskimi viri zagotavljajo takšno stopnjo varnosti. Zakaj potem sploh psevdonimizacija in anonimizacija?

Problem šifriranja se pojavi, ko je podatke treba veliko preiskovati in analizirati. V takem primeru je za vsak vpogled v podatke le-te treba vsakič znova odšifrirati, zato znajo biti takšni sistemi precej neučinkoviti. Obstaja nekaj načinov shranjevanja šifriranih podatkov, ki pripomorejo k večji učinkovitosti, kot so na primer indeksi s šifriranimi ali zgoščenimi vrednostmi določenih podatkov, ki se nahajajo v posameznem zapisu v bazi [20]. Vendarle včasih to ni dovolj, in je bolje hraniti podatke v psevdonimizirani obliki, oziroma uporabiti kombinacijo obojega. Pri psevdonimizaciji zamenjamo podatke, ki določajo posameznika, z neko vrednostjo (psevdonimom) tako, da so za identificiranje posameznika potrebne dodatne informacije. Podatki, ki določajo posameznika, morajo biti torej shranjeni nekje drugje, najbolje v

zašifrirani obliki. V kolikor pa identifikacijskih podatkov ne potrebujemo (več), jih lahko izbrišemo in tako anonimiziramo hranjene podatke. Uporabimo lahko tudi druge tehnike anonimizacije, kot je na primer generalizacija [25]. Predpostavimo, da sta trenutno identifikacijska podatka uporabnikov njihova starost in naslov bivanja. Namesto točne starosti uporabnikov bi lahko hranili le, v kateri razpon let spadajo, namesto točnega naslova pa le ulico, mesto ali državo, v kateri živijo, ob predpostavki, da ti podatki zadostujejo za namen naše obdelave. Seveda bi morali biti razponi let in širine območij, v katere razporejamo uporabnike, dovolj veliki, da zagotovimo anonimnost posameznika.

Namen obdelave osebnih podatkov skakalcev je možnost vpogleda uporabnika v dogajanje oziroma rezultate zadnjih nekaj tekem. Podatke, ki jih hranimo, obdelujemo in prikazujemo, smo omejili na tiste, ki so potrebni za podajanje informacij, ki bi si jih nek uporabnik aplikacije želel vedeti oziroma so koristne zanj. O samem skoku se hranijo sledeči podatki: čas skoka, dolžina skoka, štartna številka skakalca, serija tekme, lokacija, ter video in slika doskoka. Vsi podatki o skoku se po enem tednu od časa shranitve v podatkovno bazo (in datotečnega sistema v primeru slike in videa) izbrišejo iz sistema. Glede na naš namen obdelave podatkov smo ocenili, da daljše shranjevanje teh podatkov ni potrebno. S tem aplikacija izpolnjuje načelo omejitve shranjevanja.

Za varnost teh podatkov je poskrbljeno s šifriranjem. Do šifriranih podatkov se po shranjevanju dostopa le ob prikazu skoka na uporabnikovi napravi, kjer se prikažejo vse zbrane informacije o skoku. Iz skoraj vseh podatkov se da identificirati posameznika, zato psevdonimizacija tu ne pride v poštev. Prav tako naših podatkov ne bi bilo možno anonimizirati, v kolikor bi jih želeli uporabiti v prej naveden namen obdelave. Za šifriranje se uporablja simetrični kriptosistem AES-128 [1]. Na strani klienta, torej mobilne naprave, potrebe po šifriranju ni, saj se podatki tam le prikazujejo. Posledično se vse šifriranje in dešifriranje izvaja na strani strežnika. Za varnost prenosa podatkov med strežnikom in mobilno napravo se uporablja varna povezava

HTTPS. Tako se izognemo težavam z distribucijo ključev ali uporabi asimetričnih kriptosistemov.

6.2.1 Šifriranje z uporabo kriptosistema AES

AES je bločna šifra, torej se operacije šifriranja opravljajo na blokih podatkov [6, 17]. Kriptogram, ki ga dobimo kot rezultat šifriranja, je enake dolžine kot čisto besedilo, saj vsaka kodirna funkcija bloka bločne šifre predstavlja neko permutacijo bloka. Bloki so običajno dolgi 64 ali, kot v primeru AES kriptosistema, 128 bitov. Drug pomemben parameter bločnih šifer je dolžina ključa. Večja dolžina ključa pomeni večjo varnost, saj se skupaj z dolžino poveča število možnih ključev. Če dolžino ključa označimo z n, število možnih ključev znaša 2^n. Zmogljivosti računalnikov se vedno bolj povečujejo, temu primerno pa se vse hitreje da z izčrpnim iskanjem ključev napasti kriptosisteme s premajhnim naborom vseh možnih ključev. Da bodo podatki, zašifrirani s simetričnim kriptosistemom, varni za vsaj še nekaj časa, mora biti dolžina ključa vsaj 128 bitov [9]. Možne dolžine AES ključev so tako 128, 192 in 256 bitov. Naši podatki se ne hranijo dolgo časa, prav tako pa razkritje teh podatkov ne bi predstavljalo večjih tveganj, zato v našem primeru zadostuje uporaba ključev z dolžino 128 bitov. Za varnost pa ni dovolj le ustrezen kriptosistem, poskrbeti moramo tudi za varnost generiranega ključa. Pri šifrirnih ključih je pomembno, da se enega ključa ne uporablja v več namenov, ter da se ključe sčasoma menja, s čimer se ublaži posledice razkritja ključa. Seveda pa do razkritja ključa nebi smelo priti, zato je varna hramba ključa ena večjih skrbi pri zagotavljanju varnosti zašifriranih podatkov. V vsakem primeru se ključa ne sme hraniti poleg podatkov, ki so bili z njim zašifrirani, enako velja za hranjenje ključa v izvorni kodi aplikacije. Najbolj varno bi ga bilo hraniti na strojnih kriptografskih napravah, kot so strojni varnostni moduli (angl. *HSM - hardware security module*) [10]. Vendarle pa so te naprave drage, zato se na njih hranijo le zelo pomembni ključi, katerih razkritje bi pomenilo veliko tveganje za posameznike. Za manj občutljive podatke, kot so osebni podatki v našem primeru, se ključe običajno

hrani v datotekah na strežniku, ki jih zavarujemo z dovoljenji datotečnega sistema [8]. Najbolje je, da se nastavijo le pravice branja in še to le aplikaciji.

6.3 Pravica do informiranosti

Ker je informiranost posameznika eden glavnih ciljev uredbe, je pomembno, da je v okviru aplikacije za to poskrbljeno. Posameznik je v praksi obveščen o obdelavi podatkov na več mestih aplikacije, oziroma ob več dogodkih. Glavne informacije, ki jih mora v okviru zahtev uredbe upravljalec priskrbeti uporabnikom, so običajno zapisane v politiki zasebnosti (ang. *privacy policy*). Ker je na mobilnih napravah branje dolgih politik zasebnosti nekoliko zahtevnejše, je te informacije dobro podati v razčlenjeni obliki in v več plasteh. Dobro je ubrati pristop, kjer so skupaj podani le glavni podatki, za več informacij pa se uporabnika preusmeri na drugo stran v aplikaciji. Tu se ne sme pozabiti na tretje ponudnike storitev, o katerih mora biti uporabnik informiran. Kasneje je ob prošnjah za dovoljenje uporabe ali določenih dostopov (na primer za dostop do galerije, kamere, mikrofona, itd.) uporabnikom prav tako treba zagotoviti vse potrebne informacije. Torej, kaj točno dovoljujejo, za kaj se bodo podatki uporabljali, kako se privolitev odvzame itd.

Podatke o skokih se pridobiva od merilne naprave, torej ne neposredno od posameznikov. Glede na to, da je pravna podlaga za obdelavo podatkov privolitev, morajo biti najkasneje ob času privolitve skakalci, katerih osebni podatki se bodo obdelovali, seznanjeni s tem, kateri njihovi osebni podatki bodo v obdelavi, ter v kakšen namen se bodo zbirali njihovi osebni podatki. Prav tako bodo morali biti seznanjeni s tem, da se bodo njihovi podatki o skokih v roku enega tedna po shranitvi izbrisali, v vmesnem času pa bodo do njih lahko dostopali vsi uporabniki mobilne aplikacije.

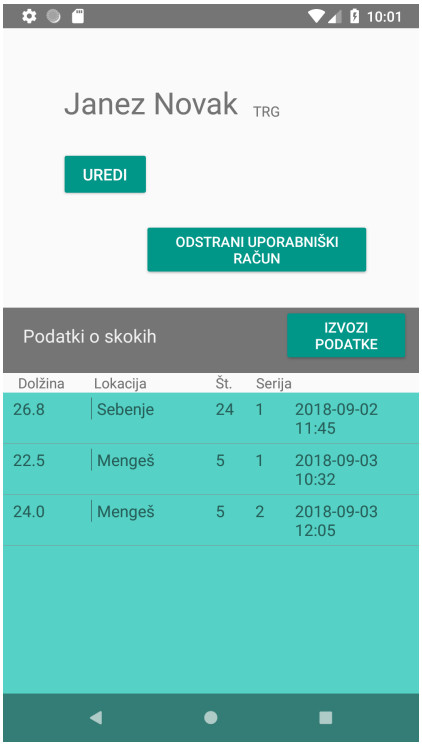
6.4 Pravica dostopa

Za izpolnjevanje pravic posameznikov je priporočljivo, da se, v kolikor je to mogoče, pripravijo učinkoviti sistemi, ki kasneje ob zahtevah posameznikov upravljalcu olajšajo delo. To so na primer aplikacijski programski vmesniki (API-ji), ki so uporabljeni tudi v naši vzorčni aplikaciji. Aplikacija tako omogoča, da z enim API klicem spremenimo podatke v bazi, dodamo zapise, jih odstranimo ... Seveda je tu treba biti pazljiv na to, kdo te klice izvaja, poskrbeti je torej treba za ustrezno avtentikacijo in avtorizacijo.

Možnost dostopa do obdelovanih podatkov posameznika je najbolje implementirati s programskim vmesnikom, saj tako posameznik lahko kadarkoli dobi vpogled v podatke, ki se zbirajo o njem. Tu je pomembna varnost izvedbe, saj lahko vsak uporabnik z uveljavljanjem te pravice dostopa le do osebnih podatkov, ki se nanašajo nanj. Posameznik lahko preko aplikacije ali pa pri administratorju dobi informacijo o tem, ali se obdelujejo njegovi osebni podatki. Uporabniki aplikacije imajo možnost dostopa do svojih osebnih podatkov prek uporabniškega vmesnika mobilne aplikacije. V kolikor je uporabnik tudi skakalec, čigar podatki se obdelujejo, se mu ob vpogledu v zbrane podatke prikažejo tudi vsi podatki o njegovih skokih. Primer takega vpogleda je prikazan na sliki 6.1. Slike in posnetke posameznik skokov si lahko ogleda s klikom na skok, pri čemer se mu prikažejo podatki, kot so na sliki 5.1. V kolikor pa skakalec ni uporabnik aplikacije, lahko dostopa do teh podatkov pri administratorju aplikacije. O možnostih dostopa mora biti skakalec obveščen še pred privolitvijo v obdelavo oziroma v času privolitve. Prav tako je ob vsaki takšni zahtevi preko pojavnega okna opomnjen o vseh informacijah o obdelavi in njegovih pravicah, ki jih lahko najde v mobilni aplikaciji.

6.5 Pravica do prenosljivosti podatkov

Pravica do prenosljivosti podatkov uporabniku omogoča pridobitev kopije vseh njegovih osebnih podatkov, ki jih upravljalec obdeluje o njem. Za iz-



Slika 6.1: Posnetek zaslona - uporabnikov vpogled v svoje podatke.

polnitev te zahteve je v aplikaciji na voljo izvoz vseh podatkov. Ob kliku na gumb za izvoz se vsi hranjeni podatki o uporabniku shranijo na zunanji pomnilnik telefona. Uredba za oblike pridobljenih podatkov definira le, da morajo biti ti v strukturirani, splošno uporabljani in strojno berljivi obliki. Takim zahtevam ustreza kar nekaj oblik zapisov, kot so na primer JSON, XML, CSV itd. Poleg samih osebnih podatkov je v nekaterih primerih dobro vključiti še metapodatke, ki podajo nekaj več informacij o podatkih samih. Seveda naj ne bodo ti metapodatki preveč specifični, saj v takem primeru prejemniku ne pomagajo in ga morda le zmedejo. V našem primeru se podatki o skokih shranijo v JSON obliki, slike in videi pa v posebnih datotekah znotraj istega direktorija. V kolikor skakalec nima uporabniškega računa v aplikaciji, za te podatke zaprosi administratorja, oziroma osebo, ki jo administrator določi kot odgovorno za obravnavo takšnih zahtev.

Naš sistem omogoča tudi prenos osebnih podatkov posameznika k drugemu upravljalcu. Upravljalcu se izda JSON spletni žeton (JWT), s katerim lahko nato prek REST API-ja na serverju pridobi podatke v odgovoru HTTP zahtevka. JSON spletni žeton je JSON objekt, ki omogoča varno izmenjavo podatkov in je velikokrat uporabljen pri avtorizaciji zahtevkov [13]. Sestavljen je iz treh delov, ločenih s piko. Prvi del je glava, ki običajno vsebuje dva podatka, tip žetona in uporabljen algoritem kodiranja. Drugi del, tovor, vsebuje poljubne podatke, ki se jih želi prenesti v žetonu. Običajno so to podatki o uporabniku, ki podaja zahtevo ali pa dodatni podatki o žetonu. Prva dva dela, ki sta zakodirana z Base64 kodirno shemo, se nato uporabi za tretji del, podpis žetona. Poleg zakodirane glave in tovora vzamemo še skrivnost in vse skupaj zakodiramo z algoritmom, ki je določen v glavi. Na ta način žeton zagotavlja integriteto vsebovanih podatkov. Ker se JWT žetoni velikokrat uporabljajo za avtorizacijo, jih moramo uporabljati v kombinaciji s HTTPS protokolom, ali pa jih je treba dodatno zašifrirati, preden se jih vključi v zahtevke.

6.6 Pravica do popravka

Mobilna aplikacija administratorju omogoča posodobitev podatkov, ki so shranjeni v podatkovni bazi. Za posamezen skok lahko posodobi lokacijo, štartno številko skakalca, dolžino skoka in serijo tekme. Slike in videa se seveda, razen izbrisa, ne da spreminjati. Podatki o skokih, ki so shranjeni v podatkovni bazi, naj bi bili pridobljeni od sistema, ki meri dolžine skokov, zato naj bi bili ti podatki natančni in pravilni. Ker pa vedno prihaja do napak, je bila dodana možnost posodobitve shranjenih podatkov. Od podatkov o skakalcu pa lahko spreminja vse – ime, priimek in skakalni klub. Administrator je dolžan popraviti le netočne in dodati le manjkajoče podatke, ne pa tudi podatkov, za katere bi posameznik želel, da bi bili pravi (na primer daljša dolžina skoka). Posameznik bo za uveljavitev pravice do popravka tako moral kontaktirati administratorja. Identifikacija posameznika, ki je podal

zahtevo, ter presoja o upravičenosti zahteve, je prepuščena administratorju aplikacije. Uporabniki aplikacije možnost posodabljanja imena in priimka najdejo v uporabniškem vmesniku pri podatkih o uporabniškem računu.

6.7 Pravica do izbrisa

Uporabnik lahko podatke o svojem uporabniškem računu odstrani sam, medtem ko podatke o skokih lahko izbriše le administrator. Izbris se v obeh primerih lahko opravi prek uporabniškega vmesnika aplikacije. Administrator ima dve možnosti izbrisa. Ena možnost je, da izbriše vse podatke o določenem skakalcu, ki so shranjeni na strežniku, ali pa le podatke skakalca, vezane na točno določeno tekmo, torej podatke o posameznem skoku. Seveda pa mora administrator pred izbrisom poskrbeti za identifikacijo osebe, ki je podala zahtevo za izbris, in se po svojih zmožnostih prepričati, da je to res oseba, na katero se nanašajo podatki, ki naj bi se izbrisali.

Vsi podatki o skokih, ki se hranijo na strežniku, se po enem tednu od shranitve avtomatsko izbrišejo, saj ni potrebe po daljšem hranjenju teh podatkov. Ker je zakonita podlaga za obdelavo podatkov o skokih privolitev, se vsi podatki o skakalcu odstranijo tudi v primeru preklica privolitve, kar skakalci lahko storijo pri administratorju.

6.8 Pravica do omejitve obdelave

V našem primeru se osebni podatki skakalcev obdelujejo le v namene, v katere je skakalec dal privolitev, zato na podlagi tega skakalec ne bi mogel doseči omejitve obdelave. Omejitev pa bi lahko dosegel ob oporekanju točnosti podatkov. V ta namen je v bazi dodan tudi stolpec, ki spremlja, ali so podatki nekega skoka aktivni ali ne. V kolikor je vrednost „false“, se podatki tega skoka ne pošljejo aplikaciji in se posledično ne prikažejo uporabnikom mobilne aplikacije. Aktivacijo in deaktivacijo zopet ureja administrator. Za uporabnike ne-skakalce je omejitev obdelave nesmiselna, saj napačne podatke

lahko popravijo, podatki pa se hranijo, dokler posameznik ne odstrani svojega uporabniškega računa.

6.9 Pravica do ugovora in pravica glede avtomatiziranega sprejemanja odločitev

Pravice do ugovora skakalec v našem primeru ne more zahtevati oziroma pravica ni potrebna, saj je podlaga za obdelavo privolitev. V kolikor posameznik ne želi, da se obdelujejo njegovi osebni podatki, lahko prekliče privolitev, v primeru uporabnika pa lahko odstrani svoj račun. Prav tako se v okviru delovanja aplikacije ne izvaja nobeno avtomatizirano sprejemanje odločitev (vključno z oblikovanjem profilov), zato tudi po tej pravici posamezniki nimajo nobene potrebe.

6.10 Evidenca dejavnosti obdelave

Aplikacija za delovanje zahteva redno obdelavo osebnih podatkov, zato je potrebno hraniti evidenco dejavnosti obdelave. Nadzorni organi nekaterih držav članic Unije [4], so na svojih spletnih straneh že objavili predloge za evidence obdelave [11, 12] v Excel in Word dokumentih, lahko pa se v ta namen ustvari tudi mikrostoritev, ki omogoča hitro posodabljanje, vpogled, preverjanje zahtev itd. V našem primeru ima vlogo upravljalca administrator aplikacije, zato mora evidenco dejavnosti obdelave voditi on, ločeno od aplikacije same.

6.11 Pooblaščena oseba za varstvo podatkov in ocene učinka v zvezi z varstvom podatkov

V našem primeru določitev pooblaščene osebe za varstvo podatkov ni potrebna, saj aplikacija ne upravlja s posebno vrsto osebnih podatkov in ne opravlja sistematičnega spremljanja posameznikov. Prav tako nam ni treba izvesti ocene učinka v zvezi z varstvom podatkov, saj obdelava ne predstavlja večjih tveganj za posameznike.

6.12 Obveščanje v primeru kršitev varstva osebnih podatkov

Obveščanje nadzornega organa o kršitvah v našem primeru ni potrebno, saj se ne zbirajo nobeni podatki, ki bi povzročali veliko tveganje za posameznike, v kolikor bi bili razkriti. Iz istega razloga kršitve ni treba sporočiti posameznikom. Poleg tega, pa so shranjeni podatki zašifrirani, in ob vdoru ne razkrijejo ničesar. Uredba v takem primeru ne zahteva obveščanja posameznikov.

Poglavje 7

Sklepne ugotovitve

Potrebi po skladnosti z GDPR-jem se je torej zelo težko izogniti. Področje veljave uredbe je zelo široko, tako geografsko, kot vsebinsko gledano. Poleg obdelovanja samih neosebnih podatkov obstaja pri možnosti izogibanja še nekaj izjem, pri katerih pa je treba biti pozoren, ali res veljajo. Aplikacije, za katere velja slednje, torej spadajo v kategorijo tistih, ki jih uredba ne zadeva. Na drugi strani pa smo definirali še večinsko kategorijo aplikacij, katerih upravljalci se pravil uredbe morajo držati. To kategorijo smo razdelili še na nekaj podkategorij. To so kategorija aplikacij, kjer upravljalec za obdelavo potrebuje privolitev posameznika, kategorija aplikacij, kjer obdelava lahko povzroči veliko tveganje, kategorija aplikacij, kjer ima podjetje oziroma organizacija upravljalca več kot 250 zaposlenih ali pa obdelava osebnih podatkov ni občasna in kategorija aplikacij, kjer osebne podatke obdeluje javni organ ali telo. Vsaka aplikacija lahko spada v več podkategorij.

Mobilna aplikacija Smučarski skoki obdeluje osebne podatke posameznikov in predstavlja primer mobilne aplikacije, skladne z uredbo. Skladnost se da preveriti po korakih. Najprej je torej treba poskrbeti za ustrezno zakonito podlago za obdelavo podatkov. V primeru mobilnih aplikacij se izkaže, da so to velikokrat privolitve posameznikov. Pri njih je treba biti pazljiv, da uporabnik ve, v kaj daje privolitev, ter da se hrani nek veljaven dokaz o privolitvi posameznika. V našem primeru je bila za obdelavo osebnih podatkov upo-

rabnikov uporabljena še druga, precej pogosta pravna podlaga, pogodbena obveznost. Ta se v primeru mobilnih aplikacij uporabi za obdelavo podatkov, brez katere uporabniki ne bi morali koristiti osnovnih funkcionalnosti aplikacije. Poleg samih funkcionalnosti mora razvijalec implementirati še varnostne ukrepe. V našem primeru smo za dodatno varnost poskrbeli s šifriranjem, ki je le eden od primerov za zagotavljanje varnosti podatkov, ki jih navaja GDPR. Za zagotavljanje pravic posameznikov je dobro implementirati tudi programske vmesnike, ki poenostavijo izpolnjevanje zahtev. Ko vemo, kako bomo ustregli zahtevam posameznikov, moramo preveriti še zahtevo po hranjenju določene dokumentacije. Uredba narekuje vodenje evidence dejavnosti obdelave in ocen učinka v zvezi z varstvom podatkov. Za obe dopušča nekaj izjem, čeprav mora evidenco dejavnosti obdelave voditi večina upravljalcev in obdelovalcev. Nekatera podjetja in organizacije so morala z veljavo GDPR določiti tudi pooblaščeno osebo za varstvo podatkov. Naša aplikacija spada v dve podkategoriji aplikacij, ki jih GDPR zadeva. Ena so aplikacije, katerih upravljalec za obdelavo potrebuje privolitev posameznika, zaradi redne obdelave osebnih podatkov pa spada še v kategorijo, ki zahteva vodenje evidence dejavnosti obdelave. Uredba pri zahtevah precej upošteva, kakšno je tveganje obdelave podatkov za posameznika, in obveščanje ob kršitvah varstva podatkov glede tega ni nobena izjema. Ob resnejših kršitvah je treba obvestiti nadzorni organ, kot tudi posameznike, na katere se nanašajo ogroženi podatki. Vsekakor je zahteve uredbe dobro upoštevati, predvsem kadar za mobilno aplikacijo stoji posameznik, saj so kazni kršenja visoke.

Literatura

[1] FIPS PUB 197, Advanced Encryption Standard (AES), 2001. U.S.Department of Commerce/National Institute of Standards and Technology.

[2] Android Developers. Dosegljivo: `https://developer.android.com/`. [Dostopano: 02. 09. 2018].

[3] 10 Best Practices for Better RESTful API. Dosegljivo: `https://blog.mwaysolutions.com/2014/06/05/10-best-practices-for-better-restful-api/`. [Dostopano: 12. 9. 2018].

[4] Data Protection Authorities. Dosegljivo: `http://ec.europa.eu/justice/article-29/structure/data-protection-authorities/index_en.htm`. [Dostopano: 2. 9. 2018].

[5] Docker Documentation. Dosegljivo: `https://docs.docker.com/`. [Dostopano: 12. 9. 2018].

[6] N. Ferguson, B. Schneier, and T. Kohno. *Cryptography Engineering: Design Principles and Practical Applications*. John Wiley & Sons, Inc., 2010.

[7] Uredba (EU) 2016/679 Evropskega parlamenta in sveta. Dosegljivo: `https://eur-lex.europa.eu/legal-content/SL/TXT/HTML/?uri=CELEX:32016R0679&from=SL`, 2016. [Dostopano: 15. 08. 2018].

[8] Guide to Cryptography. Dosegljivo: https://www.owasp.org/index.php/Guide_to_Cryptography. [Dostopano: 30. 8. 2018].

[9] ECRYPT – CSA H2020-ICT. Algorithms, Key Size and Protocols Report (2018), 2018.

[10] Hardware security module. Dosegljivo: https://en.wikipedia.org/wiki/Hardware_security_module. [Dostopano: 2. 9. 2018].

[11] Informacijski pooblaščenec. Dosegljivo: https://www.ip-rs.si/. [Dostopano: 21. 08. 2018].

[12] Information Commissioner's Office. Dosegljivo: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/. [Dostopano: 02. 09. 2018].

[13] Introduction to JSON Web Tokens. Dosegljivo: https://jwt.io/introduction/. [Dostopano: 2. 9. 2018].

[14] Java Language Specification. Dosegljivo: https://docs.oracle.com/javase/specs/jls/se9/html/jls-1.html. [Dostopano: 12. 9. 2018].

[15] Introducing JSON. Dosegljivo: https://www.json.org/. [Dostopano: 3. 9. 2018].

[16] Constantine Karbaliotis. The Nightmare Letter: A Subject Access Request under GDPR. Dosegljivo: https://www.linkedin.com/pulse/nightmare-letter-subject-access-request-under-gdpr-karbaliotis/, 2017. [Dostopano 02. 09. 2018].

[17] Lars R. Knudsen and Matthew J. B. Robshaw. *The Block Cipher Companion*. Springer Publishing Company, Incorporated, 2011.

[18] Mark Masse. REST API Design Rulebook: Designing Consistent RESTful Web Service Interfaces, 2011.

[19] European Union Agency For Network and Information Security. Privacy and data protection in mobile applications. Dosegljivo: https://www.enisa.europa.eu/publications/privacy-and-data-protection-in-mobile-applications, 2017. [Dostopano 15. 08. 2018].

[20] T. Neubauer, M. Karlinger, and J. Heurix. Pseudonymization with Metadata Encryption for Privacy-Preserving Searchable Documents. In *2012 45th Hawaii International Conference on System Sciences(HICSS)*, pages 3011–3020, 2012.

[21] Article 29 Working Party. Guidelines on consent under Regulation 2016/679. Dosegljivo: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051, 2018. [Dostopano 02. 09. 2018].

[22] PostgreSQL. Dosegljivo: https://en.wikipedia.org/wiki/PostgreSQL. [Dostopano: 12. 9. 2018].

[23] Python. Dosegljivo: https://www.python.org/. [Dostopano: 3. 9. 2018].

[24] Retrofit. Dosegljivo: https://square.github.io/retrofit/. [Dostopano: 12. 9. 2018].

[25] Personal Data Protection Commission Singapore. Guide to basic anonymisation techniques. Dosegljivo: https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Guide-to-Anonymisation_v1-(250118).pdf. [Dostopano: 30. 08. 2018].

[26] XML Essentials. Dosegljivo: https://www.w3.org/standards/xml/core. [Dostopano: 12. 9. 2018].