GAP ANALIZA ALGEBRA GRUPE SUKLADNO GDPR-u TE PRIJEDLOZI USKLAĐIVANJA U ODJELU MARKETINGA

Čop, Helena

VISOKO UČILIŠTE ALGEBRA

DIPLOMSKI RAD

GAP ANALIZA ALGEBRA GRUPE SUKLADNO GDPR-u TE PRIJEDLOZI USKLAĐIVANJA U ODJELU MARKETINGA

Helena Čop

Zagreb, svibanj 2018.

Predgovor

Pisanom izjavom posvećujem ovaj rad Miljenku Čopu i Neri Nagy, osobama koje me svakim danom iznova motiviraju i bude u meni znatiželju za shvaćanjem stvari prema kojima posjedujem strast.

Autorica smatra da tematika zaštite osobnih podataka nikada nije bila aktualnija iz razloga što je neophodno uspostaviti temelje u vidu zaštite pojedinaca, njihova prava i slobode prilikom dijeljenja istog s obzirom na količinu podataka koji su do sada bili dostupniji nego ikada. Razmatranje tematike zaštite osobnih podataka kroz pravnu prizmu i zahtjeve Uredbe može biti od koristi mnogim organizacijama koje se započinju usklađivanje u vidu primjera Algebra grupe, kroz njezine organizacijske i tehničke mjere.

Također, posebno zahvaljujem Algebra grupi i mentoru Zoranu Jančiću koji su mi omogućili uvid u svoje poslovanje, posvetili svoje vrijeme i prije svega, u dvije godine Diplomskog studija digitalnog marketinga uspješno prenijeli dio svojeg znanja i pritom potvrdili kvalitetu i stručnost u obrazovanju. To se poglavito odnosi na predmete: Marketinške strategije na internetu (doc. dr. sc Sandro Skansi), Sigurnost, privatnost i etičnost digitalnih podataka (v. pred. Nikola Protrka), i Upravljanje markom i reputacijom (pred. Tomislav Krištof). Za kraj, od srca hvala predavaču Tomislavu Krištofu koji je prepoznao moju znatiželju i strast u poslovnom svijetu i danas predstavlja mentora i prijatelja.

Sažetak

Hrvatski

Nova pravila o zaštiti osobnih podataka, Opća uredba o zaštiti osobnih podataka (Uredba) donose velike promjene u regulaciji osobnih podataka za sve pravne osobe koje u svom poslovanju obrađuju ili koriste osobne podatke. U radu je provedena Gap analiza i DPIA (engl. *Data Protection Impact Assesement*) usklađivanja sukladno zahtjevima Uredbe nad Algebra grupom. Predstavljen je dizajn programa usklađenosti za provođenje obrada i prava ispitanika s naglaskom na odjel marketinga.

Ključne riječi: Opća uredba o zaštiti osobnih podataka, osobni podatak, provođenje obrada, prava ispitanika, odjel marketinga

English:

The new rules on the protection of personal data, the Universal Declaration of Personal Data introduce major changes in the regulation of personal data for all legal entities who process or use personal information in their business. In this paper, Gap analysis and DPIA (*Data Protection Impact Assesement*) on the Algebra Group are performed in accordance with the requirements of the Regulation. The design of the compliance program for processing and the rights of the respondents with the emphasis on the marketing department was presented.

Key words: General Data Protection Regulation, personal data, processing of personal data, the rights of data subject, marketing department

Sadržaj

1. Uvod

Digitalna revolucija u potpunosti mijenja industrije, poslovne modele, neovisno o kojoj industriji je riječ, proizvodu ili usluzi. Utjecaj informacijskih tehnologija doveo je do preispitivanja starih tradicionalnih modela i njihove efikasnosti. Usvajanjem novih tehnologija, prateći nove poslovne modele utjecalo se na povećanje učinkovitosti i proizvodnosti. Upravo iz razloga agilnosti, organizacije su suočene s promjenama u okolini na koje moraju odgovoriti, efikasno i efektivno s ciljem opstanka na globalnom tržištu.

Upravo navedeno usvajanje i integracija „digitalnog“ u naše živote dovela je do toga da ljudi proizvode više podataka nego ikada prije. Podaci su postali ključan aspekt svakog poslovanja, a organizacije su svjesne kako zahvaljujući upravo tim podacima na razne načine privlače korisnike i ostvaruju dobit. Tvrtke poput Googlea i Facebooka - najveći i najmoćniji konglomerati - u poslovanju poznaju sve o svojim korisnicima, dovoljno je da uključite lokaciju na svom pametnom uređaju i Google će popratiti mjesta na kojima ste bili [1]. U posljednjem desetljeću, društveno umrežavanje je poraslo do nevjerojatnih brojki, tako Statista bilježi da su 2017. godine 71% korisnika interneta ujedno i korisnici društvenih mreža, te kako navodi, očekuje se daljnji rast [2]. Na temelju informacija koje korisnici otkrivaju bilo na društvenim mreža ili pretraživanjem na Google tražilici, rezultat je prikupljanje ogromne količine podataka na temelju kojeg se izrađuje osobni profili korisnika, što uključuje interese, kupnje, pregledavanje, povijest lokacije itd. Na taj način tvrtke mogu poduzimati akcije aktivnog ciljnog oglašavanja koje zatim korisnici prate na internetu. Kao društvo stvaramo svakodnevno ogromne količine digitalnih podataka i upravo zbog toga javila se potreba za reguliranjem privatnosti u korist korisnika s obzirom da postojeći zakoni koji upravljaju našim osobnim informacijama nisu više prikladni za svrhu. Uskoro će ta ista pravila doživjeti svoj najveći remont u dvadeset godina postojanja. Rezultat remonta je europska Opća uredba o zaštiti osobnih podataka, GDPR (engl. *General Data Protection Regulation*) koja punu primjenu započinje 25. svibnja 2018. godine. Kao takva donosi mnogobrojne promjene u načinu poslovanja organizacija koja je primjenjiva u svim zemljama EU s ciljem osiguravanja građana EU jednaku razinu zaštite osobnih podataka. Nadolazeća Uredba u potpunosti mijenja način na koji se osobni podaci trebaju prikupljati, obrađivati, koristiti i pohranjivati te na prvo mjesto stavlja pojedinca i njegovu privatnost što s pravnog gledišta do sada nije bio slučaj. Na ovaj način individualna prava zaštite osobnih podataka podiže se na novu razinu. Koji su sljedeći koraci organizacija koje moraju svoje poslovanje prilagoditi odredbama uredbi

predstavit će se na primjeru Algebra grupe, koja je kroz posljednjih 20 tak godina postala najznačajniji edukacijski partner tvrtki Microsoft, Cisco, Adobe, Autodesk, ECDL, VMware, EC-Council i drugih te obrazuje oko 18.000 polaznika seminara i programa obrazovanja godišnje, dok u visokom obrazovanju upisuju svake godine više od 200 novih studenata. U skladu sa Uredbom (EU) 2016/679 Europskog parlamenta i vijeća o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka), smjernica, mišljenja i preporuke ICO (*engl. Information Commissioner's Office*) i radne skupine iz članka 29 (engl. *Article 29 Working Party (WP29)*), evidenciji obrade osobnih podataka Algebra grupe provest će se Gap analiza koja će dati detaljan pregled u procesu usklađivanja s Uredbom te procjena učinka na zaštitu podataka koja predstavlja alat za ublažavanje rizika. Također, u radu će biti predstavljen implementacijski plan prema Gap analizi s naglaskom na odjel marketinga. Predstavljeni dizajn programa usklađenosti obuhvatiti će područje pravnih podloga za provođenje obrada i prava ispitanika. Predstavljena analiza može imati koristi za mnogobrojne organizacije koje započinju usklađivanje s Uredbom EU.

2. GDPR– „General Data Protection Regulation“

Europska direktiva pod nazivom GDPR (engl. *General Data Protection Regulation*) stupila je na snagu još 24.svibnja 2016. godine, no u punoj primjeni bit će od 25. svibnja 2018. godine.

Tehnološki napredak predstavio je potrebu za jasnijim definiranjem procesa u obradi osobnih podataka, stoga je neophodno bilo definirati novi instrument koji će osigurati zaštitu prava i temeljnih sloboda pojedinaca u vezi s obradom osobnih podataka.

U ovom dijelu predstavljena je okosnica glavnih radnji prema Uredbi, polazeći od potrebe za definiranjem osobnog podataka, posebnih kategorija osobnih podataka, načela obrade osobnih podataka te zakonitosti obrada.

S fokusom na organizacije koje imaju za cilj uspostaviti odgovarajuće procese i implementirati odgovarajuće tehničke mjere, važno pitanje koje se postavlja jest definirati što je osobni podatak. Prema Uredbi, članak 4. navodi osobni podatak: *„svi podaci koji se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi („ispitanik”); pojedinac čiji se identitet može utvrditi jest osoba koja se može identificirati izravno ili neizravno, osobito uz pomoć identifikatora kao što su ime, identifikacijski broj, podaci o lokaciji, mrežni identifikator ili uz pomoć jednog ili više čimbenika svojstvenih za fizički, fiziološki, genetski, mentalni, ekonomski, kulturni ili socijalni identitet tog pojedinca“* [3].

Uredbom se uvode nove i pojednostavljuju već postojeće definicije, definiraju se biometrijski i genetski podaci te se posebnu pozornost posvećuje posebnim kategorijama osobnih podataka, poput: rasno ili etničko podrijetlo, politička stajališta, vjerska uvjerenja, sindikalno članstvo, zdravlje ili spolni život kao i osobni podaci o kaznenom i prekršajnom postupku čija se obrada zabranjuje, osim u slučajevima definiranim, članak 9, stavka 2 koji navodi da se obrada posebnih kategorija ne primjenjuje u slučaju kada je ispitanik dao izričitu privolu s kojima se otkrivaju ti podaci te ukoliko se pravom Unije ili pravom države članice propisuje da ispitanik ne može ukinuti zabranu obrade.

Nadalje, sljedeća važna stavka propisana Općom uredbom o zaštiti osobnih podataka je obrada. Obrada prema Uredbi na temelju članka 4. predstavlja *„svaki postupak ili skup postupaka koji se obavljaju na osobnim podacima ili na skupovima osobnih podataka, bilo automatiziranim bilo neautomatiziranim sredstvima kao što su prikupljanje, bilježenje, organizacija,*

strukturiranje, pohrana, prilagodba ili izmjena, pronalaženje, obavljanje uvida, uporaba, otkrivanje prijenosom, širenjem ili stavljanjem na raspolaganje na drugi način, usklađivanje ili kombiniranje, ograničavanje, brisanje ili uništavanje" [4].

Načela po kojima se obrađuju osobni podaci zahtijevaju zakonitost, poštenost i transparentnost s obzirom na ispitanika. Naročito se pozornost pridaje ograničavanju svrhe, odnosno prikupljanju i obrađivanju podataka isključivo u skladu s navedenim svrhama te isti ti podaci moraju biti primjereni, relevantni i ograničeni na one obrade koje su nužne u odnosu na svrhe u koje se obrađuju.

Točnost kao sljedeće načelo obrade osobnih podataka navodi da podaci moraju biti točni i ažurni prema potrebi te se navodi kako se moraju poduzeti mjere radi osiguravanja točnosti podataka koji su prikupljeni sa definiranom svrhom (podaci koji nisu točni, uzimajući u obzir svrhu zbog koje se obrađuju zahtijevaju brisanje ili ispravljanje). [5].

Ograničenje pohrane podrazumijeva da osobni podaci moraju biti čuvani u obliku koji omogućuje identifikaciju ispitanika samo onoliko dugo koliko je potrebno u svrhe radi koje se osobni podaci obrađuju. Također, cjelovitost i povjerljivost su načela koja podrazumijevaju provođenje tehničkih i organizacijskih mjera s ciljem osiguravanja ispitanika od neovlaštenih ili nezakonitih obrada, gubitka, uništenja ili oštećenja prilikom provođenja mjera. Voditelj obrade ima odgovornost uskladiti se s navedenim te biti u mogućnosti dokazati usklađenost, što u ovom slučaju, prema Uredbi predstavlja pojam pouzdanosti u načelima obrade osobnih podataka.

Prema načelima obrade osobnih podataka potrebno je definirati tko je voditelj obrade, izvršitelj obrade te nadzorno tijelo u Republici Hrvatskoj sukladno Uredbi. Voditelj obrade prema članku 4. definicije je *„fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo koje samo ili zajedno s drugima određuje svrhe i sredstva obrade osobnih podataka; kada su svrhe i sredstva takve obrade utvrđeni pravom Unije ili pravom države članice, voditelj obrade ili posebni kriteriji za njegovo imenovanje mogu se predvidjeti pravom Unije ili pravom države članice"* [6]. Također, voditelj obrade ima obveze prema nacionalnom nadzornom tijelu Republike Hrvatske, Agenciji za zaštitu osobnih podataka (AZOP, Agencija) koje uključuju uspostavu, vođenje i dostavu evidencija o zbirkama osobnih podataka, pristup spisima i drugoj dokumentaciji, sredstvima obrade osobnih podataka te prilikom iznošenja osobnih podataka van Republike Hrvatske, ukoliko postoji osnova za sumnju o postojanju odgovarajuće uređene

zaštite osobnih podataka potrebno je pribaviti mišljenje Agencije. Kao što postoje obveze prema Agenciji, koja predstavlja nadzorno tijelo Republike Hrvatske, tako voditelj ima određene obveze prema ispitanicima od kojih se ti isti osobni podaci prikupljaju. Prema članku 13., stavak 1. voditelj obrade dužan je dati informacije ispitanicima prije prikupljanja osobnih podataka o:

1. *Svom identitetu*
2. *O svrsi obrade*
3. *O korisnicima i/ili kategorijama korisnika osobnih podataka*
4. *O dobrovoljnom ili obveznom davanju osobnih podataka* [7]

Također, prema članku 3. o teritorijalnom području primjene nalaže kako se Uredba odnosi na obradu osobnih podataka u okviru aktivnosti poslovnog nastana voditelja obrade ili izvršitelja obrade u Uniji, neovisno obavlja li se obrada unutar Unije ili ne. Nadalje, Uredba se također primjenjuje na obradu osobnih podataka ispitanika u Uniji koju obavlja voditelj ili izvršitelj obrade bez poslovnog nastana u Uniji, ukoliko su aktivnosti obrade povezane s nuđenjem robe ili usluga ispitanicima u Uniji, neovisno treba li ispitanik izvršiti plaćanje ili ukoliko se radi o praćenju ponašanja ispitanika dokle god se njihovo ponašanje odvija unutar Unije.

Izvršitelj obrade prema Uredbi predstavlja fizičku ili pravnu osobu, tijelo javne vlasti, agenciju ili drugo tijelo koje obrađuje osobne podatke u ime voditelja obrade. Obradu koju provodi izvršitelj obrade uređuje se ugovorom ili drugim pravnim katom u skladu s pravom Unije ili pravom države članice, koji se obvezuje prema voditelju obrade te sukladno članku 28. stavak3. navodi sljedeće:

a) *Predmet obrade*
b) *Trajanje obrade*
c) *Prirodu i svrhu obrade*
d) *Vrstu osobnih podataka*
e) *Kategoriju ispitanika*
f) *Obveze i prava voditelja obrade* [8].

Prema tome, izvršitelj obrade obrađuje osobne podatke isključivo prema uputama voditelja obrade. Također, i voditelj i izvršitelj obrade, na zahtjev surađuju s nadzornim tijelom (AZOP) u ispunjavanju njegovih zadaća. Zaduženi su, pored toga za provođenje odgovarajućih

tehničkih i organizacijskih mjera, kako bi osigurali odgovarajuću razinu sigurnosti s obzirom na rizik, uključujući aktivnosti pseudonimizacije i enkripcije osobnih podataka, osiguravaju trajnu povjerljivost, cjelovitost, dostupnost i otpornost sustava i usluga obrade, ponovnu dostupnost osobnih podataka i pristupa u slučaju incidenta (fizičkog ili tehničkog), redovno testiranje, ocjenjivanje i procjenjivanje učinkovitosti tehničkih i organizacijskih mjera s ciljem osiguravanja sigurnosti obrade. Svaki voditelj obrade odgovoran je voditi evidenciju aktivnosti obrade.

Potreba za imenovanjem službenika za zaštitu osobnih podataka (engl. *Data Protection Officer*) od strane voditelja i izvršitelja obrade sukladno članku 37. stavak 1. Uredbe pojavljuje se u trenutku kada:

1) *Obradu provodi tijelo javne vlasti, osim za sudove koji djeluju u okviru sudske nadležnosti*
2) *Osnovne djelatnosti voditelja ili izvršitelja obrade se sastoje od postupaka obrade koji zbog svoje prirode/opsega i/ ili svrha iziskuju redovito i sustavno praćenje ispitanika u velikoj mjeri*
3) *Osnovne djelatnosti voditelja ili izvršitelja obrade se sastoje od opsežne obrade posebnih kategorije podataka i osobnih podataka u vezi s kaznenim osudama i kažnjivim djelima* [9].

Ono što je ključno kod službenika za zaštitu osobnih podataka jest da djeluje samostalno, odnosno da voditelj ili izvršitelj obrade osiguraju službeniku za zaštitu osobnih podataka da ne prima nikakve upute u pogledu izvršavanja svojih zadaća te odgovara najvišoj rukovodećoj razini voditelja ili izvršitelja obrade.

Njegova pozicija uključuje eksternalizaciju, ne smije biti u sukobu interesa, primjereno educiran, uključen u donošenje odluka vezanih uz obradu osobnih podataka, neovisan od vanjskih utjecaja te kontinuirano educiran.

Zadaće službenika za zaštito osobnih podataka prema članku 39. stavak 1. uključuju:

a) *Informiranje i savjetovanje voditelja ili izvršitelja obrade te zaposlenika koji obavljaju obradu o njihovim obvezama iz ove Uredbe te drugim odredbama Unije ili države članice zaštiti osobnih podataka*

b) *Praćenje poštivanja Uredbe te drugih odredaba Unije ili države članice o zaštiti osobnih podataka i politika voditelja obrade ili izvršitelja obrade u odnosu na zaštitu osobnih podataka, uključujući raspodjelu odgovornosti, podizanje svijesti i osposobljavanja osoblja koje sudjeluje u postupcima obrade te povezane revizije*
c) *Pružanje savjeta, kada je zatraženo, u pogledu procjene učinaka na zaštitu podataka i praćenje njezina izvršavanja u skladu s člankom 35.*
d) *Suradnja s nadzornim tijelom*
e) *Djelovanje kao kontaktna točka za nadzorno tijelo o pitanjima u pogledu obrade, što uključuje prethodno savjetovanje iz članka 36. te savjetovanje prema potrebi, o svim drugim pitanjima* [10].

Prije nego li se pozicionira Uredba u poslovne procese donesen je zaključak na temelju Uredbe koje uključuju minimizaciju, odnosno opciju za što manje osobnih podataka i što manje obrada. Kako bi se postigla minimizacija osobnih podataka potrebno je uključiti pseudonimizaciju i enkripciju u poslovne procese, a kako bi se smanjila obrada potrebo je jasno definirati kako prepoznati obradu podataka u organizacijama te imati spremno održivo objašnjenje za donošenje pojedinačnih odluka u uključivanje ili isključivanje aktivnosti vezanih uz osobne podatke u registar obrada.

2.1 Pozicioniranje GDPR-a u poslovne procese

2.1.1 Analiza prilika u zaštiti osobnih podataka

Opća Uredba predstavlja produkt izazova za organizacije te potrebe koje su postavile tehnologije i globalizacija poslovanja. Usklađenost kao proces zahtijeva vremenske, financijske i potporne resurse, no pravilno provedena implementacija usklađenosti osigurava organizacijama komparativnu prednost te dugoročni povrat ulaganja. Kao takva, Uredba donosi niz prednosti no i rizika poput zastoja u poslovanju zbog neusklađenosti pa sve do utjecaja na poslovni ugled i plaćanja visokih novčanih kazni. Nova europska direktiva u potpunosti zamjenjuje Direktivu 95/46/EZ (Opću Uredbu o zaštiti podataka) te se neposredno primjenjuje u svim državama članicama EU, bez dodatne implementacije u nacionalno zakonodavstvo. Njezina najveća prednost ogleda se u transparentnosti, pružajući korisnicima usluga veću kontrolu nad svojim podacima, kao i nesmetan protok podataka unutar Unije. Iako postavlja organizacijama nove i veće zahtjeve povećava ujedno i razinu sigurnosti u svim djelatnostima, posebice za IT industriju u usklađivanju s promjenama koje nameće tehnološka digitalizacija.

2.2. Izazovi usklađivanja Algebra grupe u zaštiti osobnih podataka

Algebra grupa, vodeći hrvatski regionalni privatni obrazovni sustav, nudi svoje programe obrazovanja od 1998. godine prisutan je u 30 gradova diljem Republike Hrvatske te kao takav postao je najznačajniji regionalni partner mnogih svjetskih tvrtki poput Microsoft, Cisco, Adobe, Autodesk, ECDL, VMware, EC- Council i mnogih drugih.

Temeljem odredaba zakona o znanstvenoj djelatnosti i visokom obrazovanju Algebra grupa se sastoji od nekoliko subjekata od kojih je svaka upisana u sudski registar Trgovačkog suda u Zagrebu s definiranim djelatnostima koje obavlja, a subjekti su:

- Algebra d.o.o.
- Visoko učilište Algebra
- Pučko otvoreno učilište Algebra

S obzirom na poslovne aktivnosti Algebra grupa ima za cilj uskladiti se s Općom uredbom kroz navedene subjekte. U daljnjem tekstu predstavljeni su procesi s kojima se Algebra grupa susreće prilikom provođenja organizacijskih i tehničkih mjera. Algebra grupa koristi se kao kolokvijalni pojam i nije registrirana pravna osoba.

3. Pregled Algebra grupe

3.1 Analiza procesa privatnog obrazovnog sustava

Algebra grupa, točnije Algebra Pučko otvoreno učilište i Visoko učilište Algebra pripada tijelu s javnim ovlastima u djelatnosti visokog obrazovanja. Akreditacijsku preporuku na temelju kriterija daje neovisno stručno tijelo, Agencija za znanost i visoko obrazovanje u sustavu visokog obrazovanja i znanosti Republike Hrvatske.

Unutar Algebra grupe nalaze se tri poslovna subjekta upisana u sudski registar nadležnog suda grada Zagreba. Visoko učilište Algebra sa sjedištem u Zagrebu ima pravni oblik ustanove s definiranim djelatnostima u izvođenju studijskih programa stručnih i diplomskih studija. Osnivač subjekta je Algebra d.o.o., koja je ujedno sljedeći subjekt upisan u sudskom registru sa sjedištem u Zagrebu. Nadalje, Pučko otvoreno učilište pravnog oblika javne ustanove obavlja djelatnosti u području [11]:

- srednjoškolskog obrazovanja odraslih,
- informatičko opismenjavanje djece, mladeži i odraslih,
- proizvodnja i prodaja knjiga, audio i video materijala
- obavljanje drugih djelatnosti iz područja obrazovanja, kulture i informiranja, ponuda stranih jezika,
- usluge prevođenja
- djelatnost nakladnika
- tiskanje časopisa i periodičnih publikacija, knjiga i brošura, glazbena djela i glazbenih rukopisa, karata i atlasa, plakata, igračih karata, reklamnih kataloga, prospekata, tiskanih oglasa, djelovodnika, albuma, dnevnika, kalendara, poslovnih obrazaca pomoću knjigotiska, ofseta, fotografura, fleksografije, sitotiska i drugih tiskarskih strojeva

Jedan od načina na koje Visoko učilište Algebra provodi pouzdanost svog poslovanja ogleda se kroz zadovoljavanje visokih standarda sustava osiguravanja kvalitete koju provodi jedna od pet vodećih europskih akreditacijskih agencija NVAO [12].. NVAO je jedan od europskih autoriteta u području osiguravanja kvalitete u visokom obrazovanju.

Visoko učilište Algebra reakreditirano je s izvrsnim ocjenama i pozitivnom akreditacijskom preporukom što također dokazuje i u:

a) Kategorija „Obrazovanje“ u sklopu dodjele Microsoft godišnja nagrada za partnera – Partner of the Year Awards za 2014. godinu.
b) AZVO (Agencija za znanost i visoko obrazovanje)- najviša ocjena po četiri kriterija za znanost i visoko obrazovanje [13].

Algebra grupa u opusu svog poslovanja obrađuje i vrši obrade nužne za ostvarivanje osnovne usluge temeljem legitimnog interesa koji je pravni temelj za obradu osobnih podataka. Iako Algebra grupa ostvaruje legitimni interes potrebno je zadovoljiti uvjete u skladu s pravima EU-a.

3.1.1 Prikupljanje i obrada osobnih podataka u poslovnim procesima

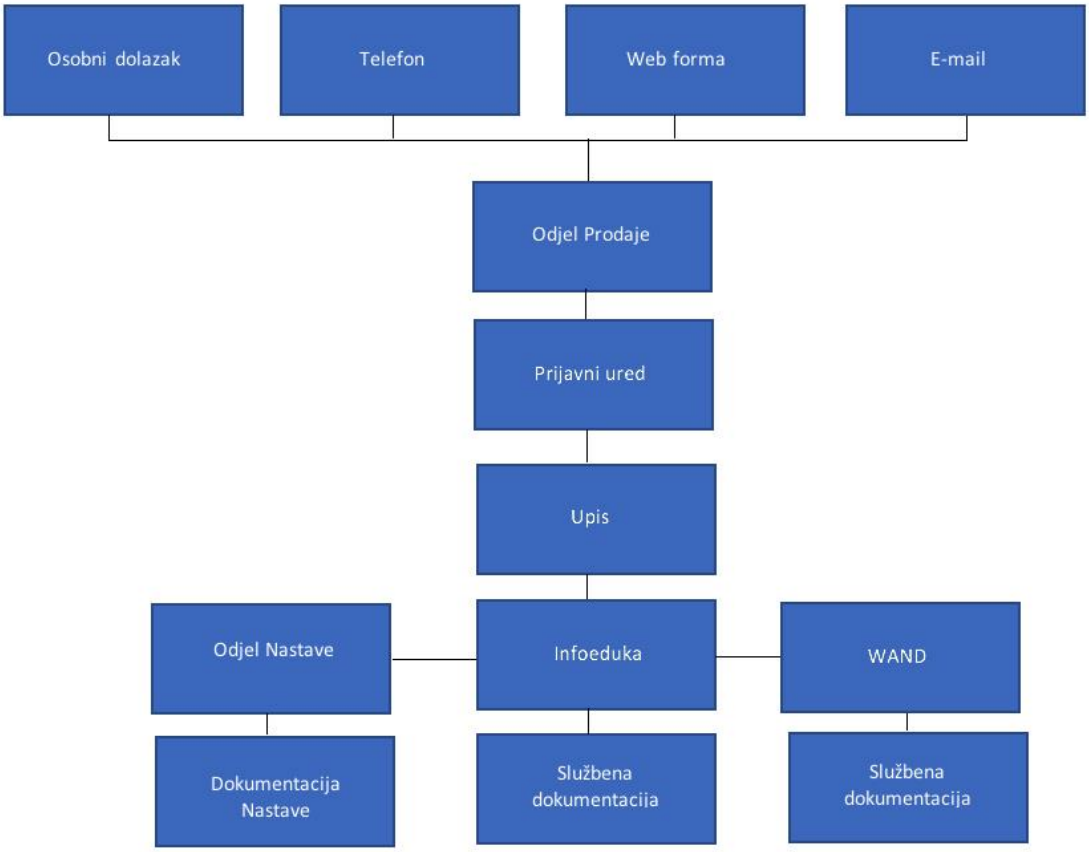
Algebra grupa u svom poslovanju obrađuje osobne podatke s obzirom na poslovnu svrhu, odnosno ukoliko postoji jasno određena i dokumentirana zakonska osnova ili osnova temeljena na ugovornom odnosu, dok su ostale obrade dozvoljene jedino uz jasnu dokumentiranu privolu vlasnika ili njegovog opunomoćenika. Preko IT sustava Algebra grupe zaposlenici vrše *„bilo automatiziranim bilo neautomatiziranim sredstvima kao što su prikupljanje, bilježenje, organizacija, strukturiranje, pohrana, prilagodba ili izmjena, pronalaženje, obavljanje uvida, uporaba, otkrivanje prijenosom, širenjem ili stavljanjem na raspolaganje na drugi način, usklađivanje ili kombiniranje, ograničavanje, brisanje ili uništavanje“* osobnih podataka [14].

U nastavku je prikazan proces protoka podataka Algebra grupe putem komunikacijskih kanala:

- telefonski kontakt,
- izravni kontakt (osobni dolazak),
- kontakt putem web obrasca
- kontakt e-mailom

s obzirom na osnovnu uslugu u koju ispitanici daju svoje osobne podatke.

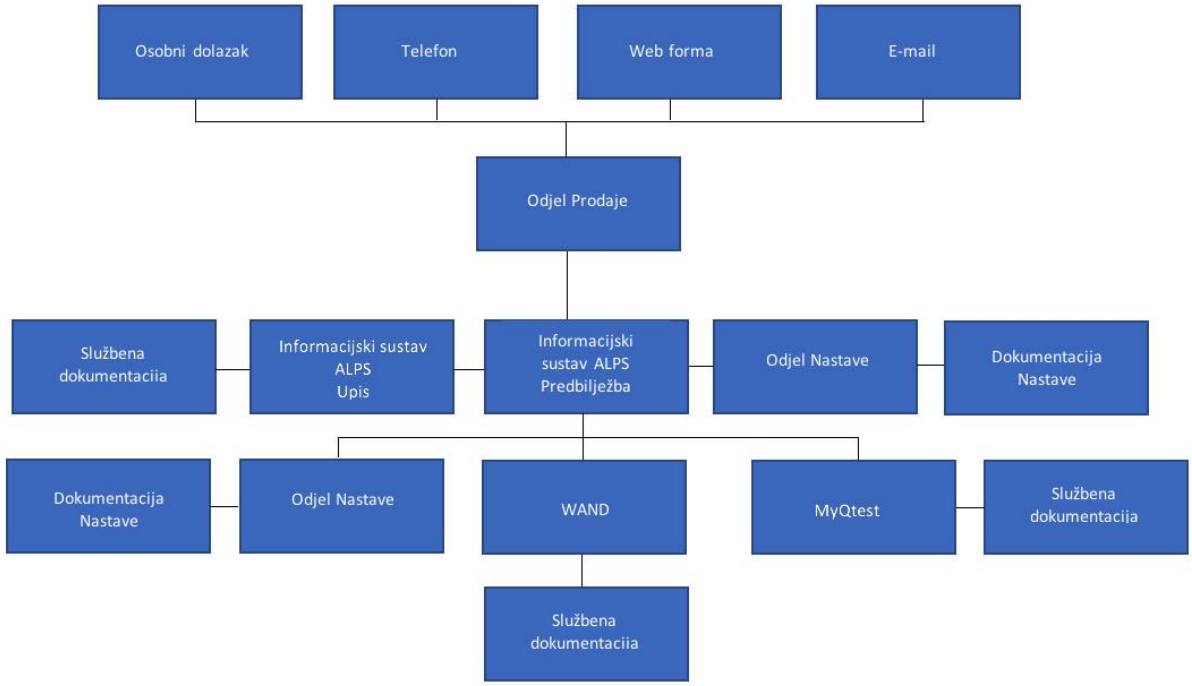
3.1.2 Prikaz kolanja osobnih podataka prema Visokom učilištu Algebra



Slika 1. Proces protoka podataka Visokog učilišta
Izvor: Autorov rad

Osobnim dolaskom, telefonom, prijavom putem web forme ili e-mailom započinje komunikacijski proces ispitanika i Visokog učilišta Algebra. Kroz navedene komunikacijske kanale Odjel prodaje obavlja prodajnu aktivnost koja se usmjerava zatim na Prijavni ured koji započinje upis osobnih podataka prema jasnoj želji ispitanika za sklapanje ugovora. Osobni podaci upisuju se u sustav Infoeduka s prijeko potrebnom dokumentacijom. Navedena aktivnost upisa ima legitimni interes, sklapanje ugovornog odnosa s polaznikom. Upisom u Infoeduku osobni podaci vidljivi su i u računovodstvenom sustavu WAND Odjela računovodstva i u Odjelu nastave koji ostvaruje pristup podacima sukladno svrsi planiranja nastave.

3.1.3 Prikaz kolanja osobnih podataka prema Pučkom otvorenom učilištu i neverificiranih programa Algebra grupe



Slika 2. Proces protoka podataka prema Pučkom otvorenom učilištu i neverificiranim programima Algebra grupe

Izvor: Autorov rad

Osobnim dolaskom, telefonom, prijavom putem web forme ili e-mailom započinje komunikacijski proces ispitanika i Pučkog otvorenog učilišta. Kroz navedene komunikacijske kanale Odjel prodaje/Prijavni ured započinje upis osobnih podataka prema jasnoj želji ispitanika za sklapanje ugovornog odnosa. Kontakt podaci polaznika upisuju se kao predbilježba – interes polaznika za ostvarivanje usluge ili direktno u informacijski sustav ALPS – prikupljanje ostalih osobnih podataka. Ukoliko je ispitanik odmah upisan u informacijski sustav ALPS, osobni podaci vidljivi su odjelu Nastave koji obavlja svoje daljnje poslovne aktivnosti vezane uz održavanje nastave s pripadajućom dokumentacijom. Uneseni osobni podaci nakon upisa u informacijski sustav ALPS odlaze u sustav WAND, odjela Računovodstva s kojim završava proces kolanja osobnih podataka s prikupljenom službenom dokumentacijom. Prikupljaju se osobni podaci nužni za ostvarenje usluge sklapanjem ugovornog odnosa između Algebra d.o.o. i fizičke/pravne ili između Algebra POU i fizičke/

pravne osobe. MyQtest ispitni je sustav kojeg koriste Algebra d.o.o i Algebra POU za testiranje polaznika edukacija, testiranje zaposlenika iz drugih firmi prema narudžbi. Identifikator je mail koji ujedno služi i kao korisničko ime s time da svaki polaznik ima jedinstveni email. Uvid u korisnike ostvaruje se prema dodijeljenim ulogama s obzirom na tip podataka unutar sustava, a pristup unaprijed definiranim podacima imaju predavači, Odjel operacija i određene osobe u Odjelu prodaje.

Također, Algebra grupa provodi neverificirane programe obrazovanja poput:

- pripreme za Državnu maturu
- MBA
- Junior (Digitalna akademija)
- Certifikacijski seminari

Proces kolanja osobnih podataka u IT sustavima isti je kao i za Algebra POU.

Osobnim dolaskom, telefonom, prijavom putem web forme ili e-mailom započinje komunikacijski proces ispitanika prema Algebra grupi u vidu sklapanja ugovornog odnosa između stranaka. Kroz navedene komunikacijske kanale osobni podaci nakon definiranja ugovorne obveze Odjela prodaje unose se u predbilježbu informacijskog sustava ALPS ili direktno u informacijski sustav ALPS putem kojeg Računovodstveni odjel izdaje izlaznu fakturu preko računovodstvenog servisa WAND. Uvid u osobne podatke ima Odjel nastave u vidu pripreme nastave i materijala za polaznike programa koju potvrđuje kroz dokumentaciju nastave. Također, osobni podaci polaznika MyQtesta vidljivi su u ALPS-u.

Sukladno članku 6. citiranog zakona, osobni podaci moraju se obrađivati pošteno i zakonito, što znači da je njihova obrada ostvariva ukoliko postoji pravni temelj i zakonita svrha. S obzirom da prikupljanje podataka u ovom slučaju ostvaruje legitimni interes i to u obliku prodaje te se prikupljaju s ciljem (u kasnijoj fazi) sklapanja ugovornih odnosa između naručitelja (primjerice Ivan Horvat) i izvršitelja (Algebra d.o.o.) u nastavku su prikazani osobni podaci koji se prikupljaju i u koje svrhe na primjeru web prijave putem obrasca za Studij digitalnog marketinga:

Visoko učilište Algebra, odnosno Odjel marketinga zaprima i sprema elektronsku prijavnicu kategorije podataka kontakt podaci/osobni podaci o klijentima/polaznicima/studentima. Osobni podaci koji se prikupljaju u svrhu ostvarivanja usluge odlaze u web bazu profitnih centara,

informacijski sustav ALPS (direktno ili kao predbilježba) te u bazu sustava za slanje *newslettera* MailChimp putem kojih prodajno osoblje kontaktira i vrši prodajne aktivnosti subjekta Visokog učilišta Algebra.

Podaci koji se prikupljaju kroz elektronsku prijavnicu su:

Ime i prezime, email, telefon, Ime škole ili fakulteta, Smjer koji me zanima, mobitel, ulica i kućni broj, poštanski broj, grad, država, JMBAG, Razred koji pohađam, Razina znanja ponuđenih područja, razine zanimanja za studije, vrste studija i količina korištenja tehnologija, Želim primati obavijesti Algebra grupe, datum rođenja.

Pristup navedenim podacima ostvaruje Odjel marketinških komunikacija i Odjel prodaje. Odjel marketinških komunikacija ostvaruje pristup navedenim podacima u svrhu kreiranja marketinških kampanja, kreiranje newslettera i ostalih marketinških i prodajnih aktivnosti koji su usklađeni s prodajnim i marketinškim strategijama Algebra grupe. Pri izradi marketinških strategija Algebra grupa koristi sve prethodno prikupljene i analizirane informacije koristeći marketinške alate Google Analytics, Google AdWords i MailChimp te eksterne izvore i istraživanja koji nisu u bazi Algebra grupe.

Ranije navedeni osobni podaci prosljeđuju se unutar poduzeća odjelima koji ostvaruju pristup ovim podacima. Podaci se prosljeđuju trećoj strani, partneru MailChimp, koji je osigurao mjere zaštite svog poslovanja sukladno zahtjevima Uredbe. Rok čuvanja osobnih podataka je trajno, a pristup backupu ostvaruje hosting tvrtka i web odjel. Također, dobiveni podaci o klijentima/ polaznicima/ studentima služe za izradu profila, koji prema Uredbi nisu mogući ukoliko se ne dobi njihova suglasnost.

Navedeni podaci nužni su za sklapanje ugovornih odnosa, no postavlja se pitanje kamo oni odlaze, tko sve unutar poduzeća ima pristup podacima u ALPS-u, CRM sustavu, Infoeduci, MyQtestu te kako se oni dalje obrađuju. U nastavku predstavljeni su IT servisi koje Algebra grupa koristi u svojim poslovnim aktivnostima.

4. IT servisi koji podupiru procese obrade osobnih podataka u poslovnim procesima

Algebra grupa u opusu svojih poslovnih aktivnosti prikuplja, obrađuje, koristi osobne podatke u vidu pružanja usluge prodaje programa obrazovanja kroz IT sustave koje koristi. Navedeni sustavi preko kojih se prikupljaju podaci su:

1. Informacijski sustav ALPS
2. MyQtest
3. Infoeduka
4. Microsoft Office Dynamics CRM

U nastavku predstavljene su zbirke prema kojima se prikupljaju osobni podaci, odjel koji ima pristup te kome se prosljeđuju osobni podaci s ciljem upoznavanja organizacijskih mjera koje je potrebno provesti kako bi se uskladili na području tehničkim mjera.

4.1 ALPS informacijski sustav

ALPS je informacijski sustav kojeg Algebra grupa (osim Visokog učilišta Algebra) koristi kroz sve subjekte u svrhu upisa i obrade osobnih podataka s ostvarenim legitimnim interesom.

Svrha prikupljanja osobnih podataka temeljena na zbirci	**Subjekt i odjel**	**Kome se prosljeđuju osobni podaci**
Uvjerenja po grupama HZZ-a	Algebra Obrazovanje odraslih, Odjel operacija	Unutar poduzeća; voditelj poslovnica, voditelj ključnih kupaca i administratori prodaje
ATES- sustav za testiranje polaznika	Alegbra d.o.o., Algebra POU, VU Algebra, Odjel prodaje	Ne prosljeđuje se
Baza podataka korisničkih domena polaznici.mojweb.com,hr (obradom podataka dobivenih iz ALPS-a)	Algebra d.o.o., Odjel marketinških komunkacija	Odjel marketinških komunikacija

Baza računa vanjskih ALPS korisnika za izradu certifikata	Algebra d.o.o., Odjel tehničke podrške	Odjel tehničke podrške
Matične knjige	Algebra POU, Odjel operacija	ASOO, prosvjetnoj inspekciji na zahtjev
Imenici i dnevnici rada	Algebra POU, Odjel operacija	Predavačima tokom izvođenja nastave
Evidencija uvjerenja	Algebra POU, Odjel operacija	ASOO, prosvjetnoj inspekciji na zahtjev
Dosjei polaznika	Algebra POU, Odjel operacija	ASOO, prosvjetnoj inspekciji na zahtjev
Sklapanje ugovora s polaznikom	Algebra POU, Odjel operacija	Unutar poduzeća, u područje dokumentacije
Evidencija predavača/ asistenata	Algebra POU, Odjel operacija	Koordinatorima kvaliteta i razvoja ljudskih potencijala, administratorima dokumentacije, djelatnicima računovodstva

Tablica 1.Prikaz evidencija obrade Algebra grupe u sustavu ALPS

Izvor: Algebra grupa

Algebra grupa prikuplja osobne podatke prema pravnoj osnovi zakona Republike Hrvatske, sukladno aktivnostima koje imaju definiran rok čuvanja te na temelju internog pravilnika Algebra grupe. Također, isti ti podaci prosljeđuju se samo unutar poduzeća i unutar Hrvatske.

4.1.1 Organizacijske i tehničke mjere usklađenosti ALPS sustava

Kako bi se uskladili sa zahtjevima Uredbe predlažu se sljedeće tehničke mjere predstavljene od tvrtke Nove Mogućnosti d.o.o. [16] koja radi na implementaciji ALPS sustava. Predložene izmjene uključuju:

- Postavljanje zapisa za polja koja definiraju kategorije podataka koji se zaprimaju

- Dodatno primanje privola iz ALPS-a

- Prima se agregirana privola koja aktivira odabrani set privola

- Primaju se privole za svaki podatak pojedinačno

- Dinamika: automatski uvoz putem integracije

- Web servis ili SQL upit za dohvat vrsta privola (*consent*) iz CRM-a

- kriptiranje svih lozinki AES256 algoritmom u CTR (*counter*) modu

U skladu s tehničkim mjerama nad sustavom potrebno je definirati i organizacijske mjere, uključujući:

- Novi popis uloga u ALPS-u prema radnim mjestima zaposlenika

(Glavni administratori, računovodstvo, voditelji ureda..)

- Raspodjela uloge *Upravitelja poslovnih prostora* na: Prodaja - backoffice, Prodaja - Infopult, Prodaja - Infopult poslovnica..

- Suglasnost za korištenje osobnih podataka integrirana je u sustav

4.2 Infoeduka

Sustav Infoeduka predstavlja digitalnu referadu koja je namijenjena studentima Visokog učilišta Algebra da ostvare informacijsko - komunikacijsku vezu s Visokim učilištem. Kroz sustav studentima su dostupne obavijesti, službeni nastavni materijali, aktualni raspored nastave te njegove izmjene. Korisničke podatke student dobiva putem elektroničke pošte prilikom prijave na studij. Korisnički podaci studenta predstavljaju i AAI identitet. Sustav AAI@EduHr je autentifikacijska i autorizacijska infrastruktura sustava znanosti i visokog obrazovanja u Republici Hrvatskoj. Svaka ustanova iz sustava Ministarstva znanosti, obrazovanja koja je uključena u sustav AAI@EduHr ima vlastitu bazu u kojoj su pohranjeni elektronički identiteti korisnika iz te ustanove. Elektronički identitet korisnik ostvaruje sve dok traje njihova povezanost s matičnom ustanovom od koje su elektronički entitet i prvotno dobili.

Sustav Infoeduka sadrži sve osobne podatke korisnika koji je upisao jedan od programa studija na Visokom učilištu. Osobni podaci koji se nalaze u sustavu temelj su legitimnog interesa kojeg Algebra grupa ostvaruje u vidu provođenja poslovnih aktivnosti obrazovnog sustava. Algebra grupa prikuplja i obrađuje one osobne podatke unutar sustava Infoeduka koji su nužni za sklapanje ugovornog odnosa, izvršavanje ugovora s Visokim učilištem, ispunjenje obveza i ostvarivanja prava ugovornih strana iz ugovora, a obuhvaća obvezne dokumente: svjedodžba o položenim ispitima državne mature, domovnica, rodni list, preslika osobne iskaznice, svjedodžbe svih razreda srednje škole (podaci o obrazovanju). Uvid u osobne podatke sustava Infoeduka imaju svi zaposlenici Algebra grupe u sklopu obavljanja svojih poslovnih aktivnosti te odgovornosti, to se posebice odnosi na Odjel upisnog pulta, Odjel prodaje i Odjel računovodstva kao i nastavnika koji imaju uvid u osobne podatke u vidu provedbe nastave i praćenja dolaznosti studenata.

4.2.1 Organizacijske i tehničke mjere usklađenosti sustava Infoeduke

S obzirom na veliki protok osobnih podataka predstavljene su organizacijske i tehničke mjere usklađivanja sustava. Sljedeće tehničke mjere predstavljene od tvrtke Nove Mogućnosti d.o.o. koja radi na implementaciji sustava Infoeduke. Predložene izmjene uključuju:

- postavljanje zapisa za polja koja definiraju kategorije podataka koji se zaprimaju

- dodatno primanje privola iz Infoeduke

- dinamika: automatski import putem integracije

- web servis ili SQL upit za dohvat vrsta privola iz CRM-a

Također, pored predstavljenih tehničkih mjera usklađenosti potrebno je definirati i organizacijske mjere koje uključuju:

- definiranje uloga (pristupa) zaposlenicima u sustav Infoeduke, ostvariti pristup samo onim zaposlenicima kojima je nužno korištenje sustava za ostvarivanje poslovne aktivnosti
- ograničiti zaposlenicima uvid u kategorije podataka

4.3 MyQtest

MyQtest je ispitni sustav kojeg Algebra grupa koristi za administraciju kompleksnog ispitnog procesa. Serverski sustav osnova je aplikacije, zadužen za generiranje pitanja, vođenje evidencije o polaznicima, vođenje naplate, administriranje korisnika, definiranje pitanja, davanje izvještaja o uspjehu korisnika. [15].

Osim za testiranja polaznika edukacija, koristi se i za testiranja zaposlenika iz drugih firmi prema narudžbi. U ovom sustavu je relativno veliki protok podataka s obzirom da se svaki tjedan održavaju ispiti, stoga su neophodne organizacijske i tehničke mjere usklađivanja.

Svrha prikupljanja osobnih podataka temeljena na zbirci	**Subjekt i odjel**	**Kome se prosljeđuju osobni podaci**
MyQtest – prikupljanje podataka o klijentima/polaznicima/studentima	Algebra POU, Algebra d.o.o., Odjel prodaje	Ne prosljeđuju se
LMS (sustav za e-učenje)- zaposlenici/korisnici/studenti/ Allianz/digitalna akademija	Algebra d.o.o., VU Algebra, odjel Razvoja	Podnosi se izvještaji menadžerima u tvrtkama unutar RH

Tablica 2. Prikaz evidencija obrade Algebra grupe u sustavu MyQtest

Izvor: Algebra grupa

Osobni podaci koji se prikupljaju u svrhu testiranja predstavljenih kategorija osoba ostvaruje legitimni interes sukladno aktivnostima koje imaju definiran rok čuvanja prema pravnoj osnovi zakona Republike Hrvatske. MyQtest je sustav koji je kompatibilan sa standardima LMS sustavima odnosno e-learning rješenjima. S obzirom na veliki protok osobnih podataka predstavljene su organizacijske i tehničke mjere usklađivanja sustava.

4.3.1 Organizacijske i tehničke mjere usklađenosti MyQtest-a

Kako bi se uskladili sa zahtjevima Uredbe predlažu se sljedeće tehničke mjere predstavljene od tvrtke Nove Mogućnosti d.o.o. koja radi na implementaciji MyQtest sustava. Predložene izmjene uključuju:

- postavljanje zapisa za polja koja definiraju kategorije podataka koji se zaprimaju

- načiniti import u DSR (engl. data source record) u DST (engl. data source table)

- načiniti uparivanje na postojeći profil ili kreiranje novog

- načiniti Excel template za import i import pravilo za uparivanje polja

- unique@fake.com

- dinamika: tjedni ručni unos

U skladu s tehničkim mjerama nad sustavom potrebno je definirati i organizacijske mjere, uključujući:

- usklađenost IT sustava i odjela Algebra grupe s privolama
- definiranje politike zaštite osobnih podataka u pravilniku Algebra grupe
- ograničavanje pristupa podacima podrazumijeva definiranje uloga – dodjelu prava pristupa osoblju u skladu s poslovnim aktivnostima

Algebra grupa predstavila je smjernice organizacijske i tehničke naravi s ciljem usklađivanja poslovanja sa zahtjevima Uredbe. Svim zaposlenicima Algebra grupe preporučuje se predstaviti dokument sa tehničkim i organizacijskim mjerama s obzirom na poslovnu aktivnost koju obavljaju u odnosu na obradu osobnih podataka. Navedene smjernice predstavljaju razumne mjere kontrole koje se odnose na IT usklađenost Algebra grupe a obuhvaćaju:

1. Kontrolu fizičkog pristupa
2. Kontrolu pristupa
3. Kontrola otkrivanja podataka
4. Sigurnu pohranu podataka
5. Održavanje, razvoj i testiranje sustava
6. Sigurno okruženje

S ciljem da se IT servisi usklade s procesima poslovanja potrebno je definirati politiku informacijske sigurnosti Algebra grupe. Potrebno je utvrditi jesu li podaci koje servisi pohranjuju nepovratno anonimizirani, obrađujemo li osobne podatke s ciljem nepovratnog sprječavanja prepoznavanja pojedinca. S obzirom da obrađujemo podatke sukladno svrsi obrazovanja potrebno je definirati procedure u vidu zaštite curenja podataka IT servisa. Nadalje, pristup osobnim podacima isključivo mora se temeljiti na stvarnoj poslovnoj potrebi, ograničen samo na one članove osoblja koji imaju odobrenje od strane voditelja obrade za

pristup podatkovnim centrima i poslužiteljskim sobama na kojima se pohranjuju osobni podaci. Potrebno je vršiti kontrolu i voditi evidenciju o pristupima.

1. Kontrola fizičkog pristupa

Fizički pristup odnosi se na pristup pojedinaca u zgradama i objektima u kojima se nalaze IT sustavi koji na bilo koji način obrađuju osobne podatke. Neki od njih mogu biti:

- aplikacijski poslužitelji
- računalni centri u kojima rade web-poslužitelji
- glavna računala i sustavi pohrane
- računala zaposlenika
- objekti u kojima se nalaze mrežne komponente i položeni kabeli
- računala za polaznike i studente

Implementacija postupaka zaštite fizičkog pristupa prema kojoj je potrebno definirati i poduzeti odgovarajuće tehničke mjere:

- sustav za otkrivanje neovlaštenog ulaska
- sustav zaključavanja

Kao i organizacijske mjere:

- zaštitar

Ukoliko se provjeravaju elektronički sustavi za kontrolu fizičkog pristupa potrebno je evidenciju o navedenom pohraniti u obliku koji omogućava provjeru do određenog roka unatrag. DPO u dogovoru s upravom Algebra grupe treba definirati rok i predstaviti ga u dokumentu informacijske sigurnosti internog pravilnika. Kako bi se zaštitili od nepravilne uporabe potrebno je vršiti redovite kontrole i voditi evidencije o navedenom.

Prema načelu minimalnog ovlaštenja potrebno je utvrditi kriterije za skupinu osoba koje imaju ovlašteni pristup područjima bitnima za sigurnost. Fizički pristup ne dopušta se nikome tko nema ovlaštenja, te sredstva koja omogućuju fizički pristup zgradama i objektima smiju se izdati samo određenim osobama koje smo ovlastili i ne smiju se prosljeđivati trećim osobama.

Nadalje potrebno je dokumentiranje upravljanjem pojedinačnih ovlaštenja za fizički pristup te uspostaviti proces podnošenja zahtjeva za:

- odobravanje
- izdavanje
- upravljanje
- preuzimanje
- vraćanje

sredstava koji omogućavaju fizički pristup ili poništenje prava fizičkog pristupa što uključuje:

- upravljanje ključevima
- vizualnim identifikacijama
- čip karticama i dr.

Potrebno je opisati pravila i postupke blokiranja ovlaštenja za fizički pristup te u onemogućiti fizički pristup i ovlaštenja za sve prostorije ukoliko pojedinac napusti tvrtku.

Nadzor prostorija nakon radnog vremena definira sljedeće:

U zgradama ili objektima u kojima su smješteni IT sustavi koji obrađuju i/ili pohranjuju osobne podatke koji se mogu povezati s osobom provodi se nadzor nakon redovnog radnog vremena.

S obzirom da se snimke videonadzora klasificiraju kao osobni podatak osjetljive prirode, potrebno je poduzeti mjere za sigurnost obrade. Prema *Zakonu o zaštiti na radu*, poslodavac smije koristiti nadzorne uređaje kao sredstvo zaštite na radu, no zaposlenici moraju biti prethodno informirani o takvoj vrsti obrade osobnih podataka na način koji je propisan u internim aktima Algebra grupe.

Potrebno je definirati:

1. Popis aktivnosti obrade koju tvrtka namjerava vršiti videonadzorom
2. Razlozi vršenja videonadzora
3. Obavijestiti osobe koje se zateknu na nadziranom prostoru - jasno označavanje objekta odnosno nadziranog prostora tako da oznaka bude vidljiva prije nego li ista osoba ulazi u prostor koji je pod videonadzorom.

Obavijest treba sadržavati sljedeće:

- predstaviti da je prostor u kojem se nalaze ili ulaze pod videonadzorom
- podatke o voditelju obrade
- kontakt podatke za ostvarivanje prava

4. Voditi evidenciju o osobama koje imaju pristup snimkama
5. Lokacije na kojima se može pristupiti u čitljivom obliku kontinuirano su nadzirane CCTV sustavom
6. CCTV sustavi ne mogu snimiti podatke gdje su vidljivi u čitljivom obliku (monitor, ispisi)

Rok čuvanja snimki jest najviše 6 mjeseci, nakon tog roka dužni smo obrisati snimke.

2. Kontrola pristupa

Ovlaštenim osobama dodijeljena su prava pristupa i služe se sustavima za obradu podataka. Ti se osobni podaci ne mogu čitati, kopirati, izmijeniti ili ukloniti bez ovlaštenja tijekom njihove obrade ili uporabe, odnosno nakon njihovog snimanja.

Cilj je u skladu s Uredbom dopustiti pristup osobnim podacima osobama koje imaju ovlašteni pristup kako bi se zaštitili podaci od manipulacije ili čitanja od strane neovlaštenih osoba.

Konceptom ovlaštenja uključuju korisnička i administratorska prava pristupu podacima u sustavu u mjeri u kojoj je to nužno za obavljanje posla sukladno funkcijama i opisu posla zaposlenika. Svako ovlaštenje za pristup mora biti povezano s ovlaštenjem za pristup podacima, povezivanjem s jednom ili više uloga utvrđenih u konceptu ovlaštenja. Osoba koja je ovlaštena za pristup podacima postupa samo u okviru koji su joj potrebni za obradu tekućeg posla prema nalogu voditelja obrade te oni poslovi za koje postoji konfiguracija u individualnom profilu ovlaštenja te osobe. Ukoliko se više korisnika nalazi u istoj bazi podataka ili se obrađuje istim sustavom za obradu podataka, prijeko potrebna je postavka logičnog ograničenja pristupa usmjerena isključivo na to da se obrada vrši za dotičnog korisnika. Ograničenost u funkciji obrade podataka nužna iz razloga minimizacije u broju funkcija potrebnih za obradu istih podataka. Osoba koja je ovlaštena pristupiti podacima također se mora identificirati i potvrditi

vjerodostojnost svog identiteta na temelju definiranih jedinstvenih faktora. Neophodno je predstaviti okvir pravila i opisati postupke za odobravanje, dodjeljivanje, poništenje i provjeravanje za pristup podacima. Prava je potrebno opisati u okviru procesa upravljanja pravima IT sustava. Ovlaštenja su povezana s osobnim korisničkim imenom (ID) i računom. Ukoliko zaposlenik napusti društvo ili prijeđe u drugi odjel, potrebno je poništiti dodijeljena prava koja je imala u vidu obnašanja dužnosti. Dokumentaciju je potrebno čuvati u roku definiranom u internom pravilniku Algebra grupe te obavijestiti sve uključene strane o napuštanju tvrtke zaposlenika, posebice administratore za IT sustave i ovlaštenja.

U području administriranja, kao i u aplikacijama treba izbjegavati koncentraciju funkcija.

Evidencija pristupa podacima nužna je o svim transakcijama, čitanja, unosa, izmjene ili brisanja. Razdoblje čuvanja evidencije ovisi o pravilima uspostavljenim s predstavnicima zaposlenika, nadležnim odgovornim osobama. Ukoliko pravila nisu definirana, rok čuvanja evidencije je tri mjeseca. Neophodni korak je zajedno s predstavnicima zaposlenika i timom za zaštitu privatnosti podataka sporazumno utvrditi nepravilnu uporabu te provoditi procjene vezane uz neželjene incidente. Potrebno je implementirati tehničke mjere zaštite putem kojih serveri zapisuju logove (zapise) pristupa i aktivnosti koje se provode nad osobnim podacima. Navedeni logovi trebaju se čuvati i analizirati u sigurnoj bazi podataka. U svim servisima koji sadrže osobne podatke potrebno je implementirati nadzor i detekciju ukoliko dođe do odstupanja od uobičajenog profila ponašanja.

Zaštita pristupa nalaže:

Pristup sustavima za obradu podataka u kojima se vrši određena aktivnost trebalo bi omogućiti u trenutku utvrđivanja identiteta osobe i nakon izvršene uspješne provjere identiteta – preko korisničkog imena i lozinke.

Provjera vjerodostojnosti identiteta definira:

Lozinke korisničkih računa moraju biti u skladu s odgovarajućim, minimalnim pravilima, u pogledu dužine i složenosti lozinke. Lozinke se moraju mijenjati u redovitim definiranim vremenskim razmacima, dok se one početne lozinke trebaju mijenjati odmah.

Potrebno je provesti zahtjeve u pogledu dužine, složenosti i valjanosti lozinke koje se osiguravaju od tehničke strane.

Zahtjevi lozinka uključuju:

- Lozinka se sastoji od najmanje 8 znakova
- Lozinka se sastoji od kombinacije znakova, prema kojem se raspoloživi znakovi dijele na četiri kategorije:
    - mala slova
    - velika slova
    - brojevi
    - posebni znakovi

Kombinacija znakova mora se sastojati od najmanje tri navedene kategorije:

- lozinka se mora mijenjati u definiranim vremenskim razmacima, najmanje jednom godišnje
- lozinka ne smije biti vidljiva na zaslonu kao običan tekst
- početna lozinka dostavlja se korisniku sigurnim kanalima i/ili se korisnika mora barem jednom potaknuti da promijeni lozinku odmah nakon prve prijave u sustav

Evidentiranje pristupa nalaže:

Svi uspješni i neuspješni pokušaji pristupa u sustave moraju se evidentirati i pohraniti u obliku koji omogućuju provjeru i tri mjeseca unatrag, a one uključuju:

- korisničko ime (ID)
- računalo
- korištena IP adresa

Blokiranje lozinki nakon neuspješnih pokušaja definira:

Pristup sustavu mora se blokirati nakon ponovljenih neuspjelih pokušaja pristupa sustavu uslijed pogrešnih *log-in* podataka. Potrebno je uspostaviti proces ponovnog postavljanja ili otključavanja blokiranih korisničkih imena (ID-a) za pristup. Korisnička imena (ID-evi) koji se ne primjenjuju dulje vrijeme, odnosno 180 dana ili rokom definiranim internim pravilnikom Algebra grupe, moraju se automatski blokirati ili postaviti u neaktivno stanje.

3. Kontrola otkrivanja podataka

Važno je osigurati da osobe koje nemaju ovlašteni pristup ne mogu čitati, kopirati, izmijeniti ili ukloniti osobne podatke tijekom elektroničkog prijenosa ili transporta, snimanja na medije za pohranu podataka te osigurati mogućnost provjere i utvrđivanja kamo će se prenijeti osobni podaci putem opreme za prijenos i koji je razlog istog.

Prijenos podataka između klijenata i poslužitelja u načelu mora biti šifriran. Šifriranje prijenosne veze jedan je od načina. Prijenos se može zaštititi protokolima SSL/TLS za mrežnu sigurnost zajedno s valjanim certifikatima u web aplikacijama - poznatim kao https protokol.

Ukoliko se osobni podaci razmjenjuju između pojedinačnih sustava unutar pozadinskog (back-end) sustava, potrebno je proučiti na koji su način pojedinačne veze zaštićene od neovlaštenog pristupa podacima. Nadalje, ako podaci ne izlaze iz osiguranog područja podatkovnog centra te ako administratori mrežnih komponenata ne mogu presretati podatke, nema potrebe za šifriranjem prijenosne veze u situacijama u kojima se zahtijevaju niske ili srednje razine zaštite. Potrebno je implementirati mjere zaštite ukoliko se osobni podaci nađu van servisa (eksportiraju u čitljivom obliku). Podaci koji zahtijevaju visoku razinu zaštite moraju se šifrirati tijekom transporta. Ukoliko se ti podaci prenose na veće udaljenosti transport mora obavezno biti šifriran. Nadalje, ako se podaci prenose na neke od vanjskih sustava šifriranje je neophodno. Sustavi u kojima se obrađuju osobni podaci moraju se zaštititi od neželjenog pristupa ili protoka podataka i od drugih mreža uporabom vatrozidova (FW-a). Bez obzira gdje su vatrozidovi implementirani, u mreži ili hardverski ili se upotrebljavaju vatrozidovi zasnovani na računalu domaćinu, oni moraju biti neprekidno aktivni. Potrebno je spriječiti da korisnik deaktivira ili zaobiđe vatrozidove.

Sigurna pohrana na prenosivim podatkovnim medijima nalaže:

Zbog visokog rizika gubitka pohrana podataka na prenosivim medijima treba izbjegavati. Ukoliko je pohrana na takvim mjestima opravdana, uporaba na tim medijima mora biti pod kontrolom, a za pohranu podataka moraju se osigurati tehničke mjere šifriranja. Svi podaci koji nisu više potrebni trebaju se obrisati.

Dokumentiranje i kontrola procesa nad podatkovnim medijima nalaže:

Potrebno je kvalificirati sustav kojim će se upravljati podatkovnim medijima. Dokumentacija treba sadržavati količinu podatkovnih medija koji sadrže osobne podatke, u koju svrhu i poslove su kreirani, postupci obrade i mjesto gdje se čuvaju do trenutka njihovog uništenja te navesti kopije ukoliko postoje koje se čuvaju u trajanju od tri mjeseca ili prema pravilniku Algebra grupe nakon prestanka zaduženja ili aktivnosti. Neophodno je vršiti kontrolu nad zalihama podatkovnih medija. Ukoliko podatkovni mediji sadrže osobne podatke potrebna je visoka kontrola sigurnosti nad njima.

Sigurnost čuvanja podatkovnih medija nalaže:

Dobiveni ili dohvaćeni osobni podaci spremaju se u sigurnosne ormariće, podatkovne sefove ukoliko postoji potreba zaduženja ili aktivnosti obrade.

4. Sigurna otprema podataka, uvođenje i implementacija propisa o otpremi

Ukoliko se osobni podaci otpremaju na podatkovnim medijima, postoji propisi o pakiranju i otpremi. Osobni se podaci prije transporta moraju šifrirati, navesti ovlaštene osobe, dokumentirati transport u skladu s načelom dvostruke kontrole.

Sigurno brisanje, odlaganje i uništavanje nalaže:

Potrebno je uspostaviti i opisati procese prikupljanja, odlaganja, uništavanja ili brisanja neelektroničkih podatkovnih medija i informacijskih medija. Također, organizacija treba opisati pravila i postupke za sigurno prikupljanje i interno prosljeđivanje, pohranu i uništavanje medija. Samo proces uništavanja ili brisanja podataka provodi se pravovremeno na radnoj stranici kako bi se u velikoj mjeri izbjegla pohrana privremenih medija. Na taj način postiže se ograničenost u rukovanju podatkovnim medijima te se postiže veća sigurnost. Nadalje, potrebno je poduzeti organizacijske mjere kako bi se isključili alternativni načini odlaganja. Potrebno je vršiti kontrolu nad zaposlenicima.

Nešifrirani podatkovni mediji iz sigurnosnih razloga moraju se brisati sukladno pravilima o zaštiti podataka prije njihove ponovne interne uporabe ili prosljeđivanja vanjskim stranama. Formatiranje nije prikladan način sigurnog brisanja, potrebno je odabrati načine brisanja/uništavanja kojim se iznimno otežava rekonstrukcija podataka.

Također, trajno brisanje podataka i nosača podataka s osobnim podacima sukladno pravilima uredbe mora se evidentirati. Evidencija treba biti pohranjena u obliku koji omogućuje provjeru najmanje tri mjeseca unatrag ili prema internom pravilniku Algebra grupe. Neophodna je i kontrola unosa, u kojoj se nakon izvršene radnje mora osigurati provjera i sa sigurnošću utvrditi jesu li osobni podaci uneseni u sustave za obradu podataka izmijenjeni ili uklonjeni, te ukoliko jesu potrebno je učiniti kontrolu unosa osobe koja je to učinila. Unos u sustav za obradu osobnih podataka evidentira se, a evidencija se čuva tri mjeseca ili prema internom pravilniku Algebra grupe.

5. Održavanje, razvoj i testiranje sustava

Potrebno je ustanoviti i ograničiti da su osobni podaci u čitljivom obliku dostupni trećim stranama ili lokalnom osoblju koje održava aplikacije i IT infrastrukturu. Prilikom testiranja/ promjena/prilagodbe sustava organizacija mora uspostaviti procedure i mehanizme za anonimizaciju, enkripciju i pseudonimizaciju. Ukoliko se pojavi promjena u sustavu moraju biti uspostavljene mjere i procedure za identifikaciju rizika. Preporuča se korištenje tehnika de-identifikacije koja preuzima podatke iz proizvodnog sustava i pretvara ga u neosjetljive podatke koji su prikladniji za ispitivanje ili analizu. U skladu s kontrolom upravljanja ključevima u svrhu održavanja i zaštite sustava potrebno je provjeriti nalazi li se enkripcijski ključ van koda.

6. Sigurno okruženje

Potrebno je implementirati tehničke mjere zaštite enkripcije u računalnoj mreži te osigurati da se enkripcijski ključevi čuvaju trajno. Unutar organizacije definirati procese koji osiguravaju redovito ažuriranje protokola komunikacije, enkripcijskih algoritma i duljinu ključa. Važno je vršiti redovitu kontrolu na postojeće ranjivosti u IT servisima te definirati vrijeme i točku oporavka sustava u slučaju katastrofe te sve navedeno dokumentirati u evidenciji o sigurnosti nad osobnim podacima.

5. Implementacijski plan

5.1 Dizajn programa usklađenosti GDPR-a u poslovne procese organizacijske strukture Algebra grupe – procjena rizika u obradi osobnih podataka

S obzirom na omogućeni uvid u postupke nad osobnim podacima, bilo automatiziranim ili neautomatiziranim sredstvima u nastavku je predstavljena Gap analiza Algebra grupe sukladno zahtjevima Uredbe. Predstavljena je analiza poslovnih procesa, preporuke i usklađenost Algebra grupe te potreba za provođenjem procjene rizika kroz DPIA (engl. *Data Protection Impact Assessment*).

Procjena učinka na zaštitu podataka (engl. *Data Protection Impact Assessments*; DPIA) koristi se za identifikaciju i ublažavanje rizika vezanih uz zaštitu podataka koji proizlaze iz postojećih ili novih projekta što ima veliki utjecaj za organizaciju općenito. Ispitanici čije osobne podatke organizacija prikuplja, pohranjuje, koristi izloženi su rizicima. Upravljanje rizicima od iznimne su važnosti u vidu smanjenja negativnog učinka na privatnost, prava i slobode pojedinaca. Upravo iz tog razloga, DPIA je nužan za upravljanje rizicima kroz organizacijske i tehničke mjere kako bi se dokazala sukladnost s GDPR-om.

Provođenje DPIA poboljšat će svijest o organizaciji o rizicima nad podacima o ispitanicima povezanih s uslugom koju nudite. Provođenje DPIA donosi prednosti:

1. Osigurava i dokazuje da organizacija usklađena s GDPR-om te izbjegava sankcije
2. Potiče povjerenje u javnosti poboljšanjem komunikacija o pitanjima zaštite podataka
3. Osiguravanje da vaši korisnici nisu u opasnosti od kršenja prava na zaštitu podataka
4. Omogućite organizaciji uključivanje *data protection by design* u nove projekte
5. Smanjenje operativnih troškova optimizacijom tokova informacija unutar projekta te eliminiranje nepotrebna prikupljanja i obrade podataka
6. Smanjenje rizika vezanih uz zaštitu podataka u organizaciji [17]

Postavlja se glavno pitanje treba li se provesti DPIA, odnosno je li on nužan za usklađivanje s Uredbom o zaštiti osobnih podataka. Prema članku 35. GDPR-a, provedba DPIA je nužna od strane voditelja obrade podataka kada postoji vjerojatnost da će neka vrsta obrade osobnih podataka predstavljati veliki rizik za prava i slobode pojedinaca. Provedba DPIA ne utječe na smanjenje rizika samo od sebe, no pomaže u identifikaciji prijetnji i pronalaženja načina

ublažavanja rizika u ranoj fazi, tehničkim i organizacijskim mjerama. Učinkovita provedba aktivnosti uključuje dokumentiranje:

- vrsta prikupljanih osobnih podataka
- načini prikupljanja, obrade, korištenja, prenošenja (ukoliko postoje) i pohranjivanja podataka
- svrhu i način dijeljenja podataka među poslovnim entitetima
- tehničke mjere sigurnosti koje se primjenjuju s ciljem sprječavanja neovlaštenog pristupa podacima prilikom svake obrade

Nužno je, kako bi se organizacija uskladila s zahtjevima provesti analizu utjecaja, s usmjerenjem na one obrade osobnih podataka koje bi kao što je već spomenuto, mogle izložiti ispitanike, njihova prava i slobode visokom riziku. U analizi DPIA potrebno je analizirati tijek informacija kako bi se utvrdili tipovi podataka koji su predmet obrade i način na koji se ti podaci obrađuju. U analizi tijeka informacija potrebno je identificirati sljedeće elemente:

- utvrđivanje vanjskih i unutarnjih sudionika u postupcima obrade
- opis uloga sudionika u procesima kolanja podataka
- identifikacija elemenata osobnog podatka (format, lokacija spremanja ukoliko ga ima, struktura)
- tehnike kojima se obrađuju osobni podaci
- ostali zakonski zahtjevi u obradi podataka

Prema uputama ICO (*Information Comissioner Office*) predstavljena je procjena učinka nad svim obradama koje provodi Algebra u sklopu nuđenja obrazovnih programa :

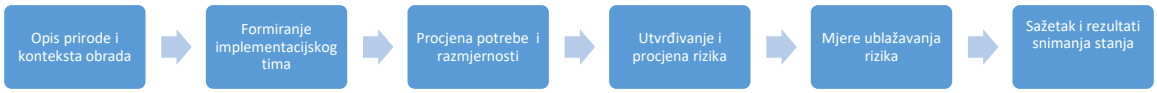
- Visoko učilište Algebra (stručni studiji)
- obrazovanje odraslih (programi obrazovanja i seminari)
- certifikacijski seminari (informatički certifikati)
- pripreme za Državnu maturu (neverificirani programi)
- MBA (postdiplomski studijski program)
- Junior (neverificirani edukacijski program; Digitalna akademija)

Ovaj dokument predstavlja *Procjenu utjecaja na zaštitu podataka (DPIA)* koja procjenjuje upotrebu i svrhu korištenja osobnih podataka u vidu procjene rizika nad Algebra grupom. DPIA je analiza očekivanih aktivnosti povezanih s procjenom i obuhvaćanjem detalja same

aktivnosti obrade i procjenu rizika povezanih s obradama, uključujući sve mjere koje je potrebno poduzeti kako bi se ublažili rizici.

DPIA se provodi zbog zahtjeva koje donosi članak 35. GDPR-a, gdje bi obrada vjerojatno mogla rezultirati visokim rizikom za prava i slobode fizičkih osoba, te potrebe da voditelj obrade provodi procjenu utjecaja predviđenih obrada.

U ovom dijelu DPIA predstavljen je sistematski opis predviđenih procesa operacija u skladu sa zahtjevima Algebra grupe prilikom prikupljanja osobnih podataka u svrhu nuđenja osnovne usluge za koju ostvaruje legitimni interes – nuđenja i prodaje programa obrazovanja. Koraci pri implementaciji Uredbe u poslovne procese Algebra grupe su kako slijedi:



Slika 3. Procesi operacija usklađivanja Algebra grupe prema DPIA
Izvor: Autorov rad

Procjena ima vrijednost za pojedince, organizacije i društvo općenito. Ovaj DPIA procjenjuje rizike za privatnost procesa procjene te identificira potrebu za organizacijskim i tehničkim mjerama zaštite i mehanizma s ciljem ublažavanja tih rizika te identificira hoće li nužnost obrade osobnih podataka uravnotežiti prava privatnosti prikupljanja i obrade podataka.

Glavne informacije		
(a)	Voditelj obrade	Algebra grupa (Algebra Pučko otvoreno učilište, Visoko učilište Algebra i Algebra d.o.o.)
(b)	Opis projekta	Ova procjena utjecaja obuhvaća izradu, isporuku i izvještavanje o procjenama tvrtke Algebra d.o.o. u usklađivanju s zahtjevima Uredba (EU) 2016/679 Europskog parlamenta i vijeća, *Zakona o zaštiti osobnih podataka* u vidu specificiranja uvjeta pod kojima je obrada osobnih podataka zakonita.
(c)	Svrha projekta	- **Politika kontrole pristupa** (Ograničavanje pristupa informacijama, dodjela prava pristupa) - **Upravljanje privolama** (vođenje evidencija svih ispitanika, aktivnih i neaktivnih privola, zahtjevi ispitanika vezano uz privole i obradu njihovih podataka sukladno pravima koje nalaže Uredba)
(d)	Kontekst, opseg i pozadina	Prikupljanje, obrada, korištenje, uvid u osobne podatke u vidu pružanja usluga programa obrazovanja kroz IT sustave : - informacijski sustav ALPS - MyQtest ispitni sustav - CRM (Microsoft Office Dynamics system) - Infoeduka Prikupljanje podataka u marketinške svrhe: - MailChimp - Google Analytics
(e)	Subjekti podataka (pod nazivom "Sudionici" u ovom dokumentu)	Procjene se dostavljaju: - zaposlenicima - dobavljačima - partnerima

(f)	Tipovi osobnih podataka	U IT sustavima prikupljaju se podaci koji su nužni za ostvarivanje usluga prema : - Zakonu o obrazovanju odraslih (NN broj 17/07) - Pravilniku o javnim evidencijama (interni pravilnik Algebra POU) - Zakon o radu (NN broj 127/17) - Zakon o zaštiti na radu (NN broj 71/14) - Zakon o računovodstvu (NN broj 120/16) - Zakon o arhivskoj građi (NN broj 12/67) Prikupljaju se osobni podaci kategorija osoba: - klijenti - polaznici - student - zaposlenici Prema kategorijama podataka: - kontakt podaci/osobni podaci
(g)	Posebne kategorije osobnih podataka	Ne prikupljaju se
(h)	Primatelji osobnih podataka: tko će moći vidjeti i imati pristup rezultatima procjene	Tim: Implementacija usklađenosti sa zahtjevima Uredbe: - DPO - Razvojni tim - Uprava (ukoliko bude potrebno)

Tablica 3. Procjena rizika za privatnost procesa Algebra grupe

Izvor: Autorov rad

Utvrđivanje i procjena rizika

Opišite izvor rizika i prirodu potencijalnog utjecaja na pojedince	**Vjerojatnost štete (malo vjerojatni, mogući ili vjerojatni)**	**Ozbiljnost štete (Minimalna, značajna ili ozbiljna)**	**Sveukupni rizik (mali, srednji, veliki)**
Prijavnice na web stranici, osobni podaci prikupljaju se elektronski i izrađuju profili koji imaju potencijalno veliki utjecaj na pojedince	Mala vjerojatnost štete (pitanje jesu li ti svi podaci koji se prikupljaju potrebni za prijavu, kamo odlaze, tko ima pristup u sustavima te postoji li privola za svrhu profiliranja)	Značajna šteta	Mali rizik
Prikupljanje podataka telefonskim putem, potreba za sigurnosnim mjerama putem maila	Mala vjerojatnost	Minimalna šteta	Mali rizik
IT Sustavi Algebra grupe, ukoliko nad sustavima nisu provedene sigurnosne tehničke kontrole utjecaj na pojedince očituje se kroz pristup informacijama od strane svih zaposlenih (potreba za ograničavanje pristupa) i curenja podataka	Moguća	Značajna šteta	Srednji rizik
Izmjena i dopuna pravilnika o radu, politika zaštite osobnih podataka (redizajn ugovornih odnosa sa partnerima i dobavljačima)	Vjerojatna	Značajna	Srednji rizik
Neusklađenosti zbirki obrazaca	Vjerojatna	Značajna	Srednji rizik

Tablica 4.Utvrđivanje i procjena rizika Algebra grupe

Izvor: Autorov rad

Mjere ublažavanja rizika

Rizik	**Opcije smanjenja ili eliminacije rizika**	**Utjecaj na rizik (elimininiran, smanjen ili prihvaćen)**	**Preostali rizik (mali, srednji, visok)**	**Odobrene mjere (Da/ Ne)**
Prijavnice na web stranici, osobni podaci prikupljaju se elektronski i izrađuju profili koji imaju potencijalno veliki utjecaj na pojedince – mali rizik	Eliminacija rizika privolom s predstavljenom svrhom obrade	Elimininiran	Mali	Da
Prikupljanje podataka telefonskim putem, potreba za sigurnosnim mjerama putem maila	Smanjenje rizika definiranjem role u Infomailu (ograničavanje uvida)	Prihvaćen	Srednji	Da
IT Sustavi Algebra grupe, ukoliko nad sustavima nisu provedene sigurnosne tehničke kontrole utjecaj na pojedince očituje se kroz pristup informacijama od strane svih zaposlenih (potreba za ograničavanje pristupa) i curenja podataka	Smanjen rizik definiranjem role u IT sustavima	Prihvaćen	Srednji	Da
Izmjena i dopuna pravilnika o radu, politika zaštite osobnih podataka i informacijske sigurnosti	Redizajn ugovornih odnosa sa partnerima i dobavljačima	Prihvaćen	Visoki	U procesu

Tablica 5. Mjere smanjenja rizika Algebra grupe

Izvor: Autorov rad

5.2 Gap analiza Algebra grupe

Izvršenje programa usklađenosti poslovnih procesa u organizacijsku strukturu Algebra grupe procijenjena je sukladno zahtjevima Uredbe te je predstavljena u Gap analizi pod nazivom Usklađenost Algebra grupe.

5.2.1 Načela zaštite podataka

Novi zahtjevi	**Značajne promjene**	**Što je potrebno da bi se uskladili?**	**Usklađenost Algebra grupe**
1. Načela zaštite podataka Načela po kojima se vodi pravo na zaštitu osobnih podataka: · pravednost, zakonitost i transparentnost · ograničenje svrhe · minimiziranje podataka · kvaliteta podataka · sigurnost · integritet i povjerljivost Novi zahtjevi donose odgovornosti za Službenika za zaštitu osobnih podataka koji moraju dokazivati usklađenosti s načelima uredbe.	Ne	1. Pregledati i revidirati trenutne politike zaštite osobnih podataka, kodekse ponašanja te proći kroz obuku zaposlenika kako bi bili sigurni da su usklađeni s izmijenjenim načelima. 2. Provesti informacijsku reviziju kako bi razumjeli gdje se podaci drže, u kojem obliku, koje su točke prikupljanja, osnova za njegovu obradu (privola/ pravni temelj) 3. Potrebno je utvrditi način za dokazivanje sukladnosti. Kako ispunjavamo uvjete, pratimo kodekse ponašanja, gdje su definirane odluke o obradi osobnih podataka te po potrebi procjena utjecaja na privatnost.	1. Politike i kodeksi ponašanja u procesu su redizajna, a zaposlenici su upoznati s zahtjevima kroz video koji je izrađen u interne svrhe. 2. Lokacije čuvanja podataka elektronski: - Cloud (Office 365) - lokalno - informacijski sustav ALPS - baze predavača - Wordpress - vanjska platforma - uređaji za snimanje (videonadzor) - O365 shared mailbox/ Sharepoint Lokacije čuvanja podataka papirnato: - unutar Algebra grupe Točke prikupljanja podatka:

		4. Pregledati Uredbu koja definira dob u obradi osobnih podataka prilikom obrade, ukoliko postoji obrada 5. Osigurati da se nadzornom tijelu (AZOP) dokaže usklađenost s Uredbom (postignute odluke o načinu i korištenju podataka u svrhe)	- izravni kontakt - e- mail - telefonski poziv - pismeno od kandidata - putem web obrasca - ALPS - DVR sustav Osnova za obradu: - legitimni interes - izvršavanje osnovne usluge - Zakon o obrazovanju odraslih - Zakon o javnim evidencijama - Zakon o zaštiti na radu/Zakon o radu - ugovor o školovanju - Zakon o računovodstvu - Zakon o arhivskoj građi Osnova za obradu: - privola ispitanika 3. Uvjeti se ispunjavaju sukladno zakonima ovisno o usluzi, prate se kodeksi ponašanja i odluke o obradi osobnih podataka koje su regulirani internim aktom, procjena utjecaja na privatnost kroz ažuriranje IT sustava 4. Obrada osobnih podataka djece s obzirom na uslugu Digitalne akademije, kreirati privolu u te svrhe koju ispunjava

			nositelj roditeljske odgovornosti 5. Evidencija aktivnosti obrade ne dostavlja se nadzornom tijelu već se daje nadzornom tijelu na uvid prilikom obavljanja nadzornih aktivnosti.

5.2.2. Zakonitost obrade

Novi zahtjevi	Značajne promjene	Što je potrebno da bi se uskladili?	Usklađenost Algebra grupe
2. Zakonitost obrade Postavljena su nova ograničenja u vezi s korištenjem suglasnosti i obradom podataka. Postoje određena ograničenja za oslanjanje na *„legitimne interese“* kao osnove za obradu te pojašnjenja kako se oni mogu koristiti. Postoji niz faktora prema kojima će se određivati je li obrada podataka za novu svrhu nespojiva s namjenom za koju su podaci prvotno prikupljeni.	Da. Privola je restriktivnije naravi. Članak 6. stavak 1. f navodi da je obrada nužna za svrhu ostvarivanja potreba legitimnih interesa .	1. Osigurati jasnoću nad osnovama za zakonitu obradu u okvirima uredbe 2. Pregledati ugovore o razmjeni informacija – oslanjanje na legitimne interese ukoliko postoje, napraviti izmjene koje ukazuju na odgovarajuću zakonodavnu osnovu ili suglasnost (privolu) 3. Prilikom definiranja privola, osigurati kvalitetu pristanka oslanjajući se na ispunjenje zahtjeva prema dobrovoljnoj, posebnoj, informiranoj i nedvosmislenoj privoli	Osigurano kroz zakonske akte države članice, internim pravilnikom, privolama, drugim izvršiteljima usluga za Algebra grupu kroz ugovorne klauzule. Privole ispitanika specificirane su u dijelu: *4.1.3 Pravna podloga za provođenje obrada sukladno: Zakonima, Ugovornim odnosima i privolama*

5.2.3. Privola/ suglasnost

Novi zahtjevi	Značajne promjene	Što je potrebno da bi se uskladili?	Usklađenost Algebra grupe
3. Privola/ suglasnost Privola podliježe dodatnim uvjetima u okviru Uredbe. - Ne preporuča se prema Uredbi da privola bude uvjetovana uslugom - Privola također mora biti odvojena od drugih pisanih sporazuma, jasno predstavljena i lako opozvana s obzirom na prava ispitanika	Da. Članak 4. definicija navodi privolu kao *„dobrovoljno, posebno, informirano i nedvosmisleno izražavanje želja ispitanika kojim on izjavom ili jasnom potvrdnom radnjom daje pristanak za obradu osobnih podataka koji se na njega odnose“* Recital 25 prema ICO smjernicama [18] sugerira da privola bude predstavljena: *"Označavanje okvira prilikom posjeta ... web stranici, odabiru tehničkih postavki ... ili bilo kojom drugom izjavom ili ponašanjem koje jasno ukazuje ... prihvaćanje predložene obrade njihovih podataka. Tišina, unaprijed označene kutije ili neaktivnost ne bi smjela biti suglasnost. "* Izričito je suglasnost još uvijek	Kada je suglasnost u pitanju potrebno je osigurati da pristanak predstavlja osnovu za zakonitu obradu: - Pristanak je aktivan i ne oslanja se na šutnju, neaktivnost ili unaprijed označene *check boxove* - Pružanje usluge ne smije biti uvjetovano označavanjem *check boxa* - Ispitanik se obavještava da ima pravo povući suglasnost u bilo kojem trenutku, no to neće utjecati na zakonitost obrade temeljem pristanka prije njegova povlačenja - Metode	Osobni podaci prikupljaju se sukladno privoli u: - marketinške svrhe - prodajne svrhe - svrhe profiliranja korisnika Privole su predstavljene i opisane s obzirom na svrhu te je ponuđen korisniku odabir komunikacijskog kanala putem kojeg želi ostvarivati komunikaciju s Algebra grupom. Privole su u skladu s preporukama zahtjeva Uredbe. Nad IT sustavima Algebra grupe integrirana je privola s jasno definiranim komunikacijskim kanalima koje je ispitanik odabrao. Također, u sustavu Infoeduke onemogućen je pristup svim studentima

	potrebna za opravdanje obrade osjetljivih / posebnih kategorija osobnih podataka, osim ako postoje drugi zakonodavni uvjeti (uključujući pružanje skrbi ako je podrazumijeva pristanak, život ili smrt itd.).	povlačenja suglasnosti nalaze se na istom mjestu gdje je prvotno tražena privola - Organizacija se ne oslanja na privolu u kojoj postoji neravnoteža između nositelja podataka i voditelja obrade (posebice ako je voditelj javni organ) - Definirati kako je proveden i pohranjen pristanak, kako korisnici mogu povući suglasnost te kako je regulirano i usklađeno u IT sustave.	do trenutka potpisivanja ugovora o suglasnosti nad korištenjem osobnih podataka s jasno predstavljenom svrhom koja je u skladu sa zakonskim aktima nadležnog tijela u obrazovnom sustavu, AZVO.

5.2.4. Djeca

Novi zahtjevi	Značajne promjene	Što je potrebno da bi se uskladili?	Usklađenost Algebra grupe
4. Djeca Djeca su identificirana kao "ranjive osobe" i zaslužuju "specifičnu zaštitu". Ukoliko se djeci pružaju mrežne usluge, a za postizanje zakonitosti obrade njihovih podataka potrebna je privola, suglasnost se mora dati ili dobiti od ovlaštene osobe koja ima roditeljsku odgovornost za dijete. se odnosi na djecu mlađu od 16 godina.	Predstavljeni zahtjevi Uredbe ne sadrže posebna ograničenja u obradi podataka o djeci, a pravila o sposobnosti djeteta definiraju nacionalni zakoni. Prema članku 8. Uredbe u kojoj se zahtijeva pristanak roditelja u pogledu nuđenja informacijskog društva izravno djetetu, obrada osobnih podataka djeteta zakonita je ukoliko dijete ima najmanje 16 godina i dao je privolu ili je odobreno od nositelja roditeljske odgovornosti nad djetetom. Također, države članice mogu u te svrhe predvidjeti nižu dobnu granicu, no ne nižu od 13 godina. Nadalje, voditelj obrade dužan je prema članku 8. (1a) uložiti „razumne napore“ kako bi provjerio odobrenje – je li dano ili odobreno od strane nositelja roditeljske	1. Ukoliko se nude, kako akt opisuje „usluge informacijskog društva izravno djeci“ 2. Izvršiti procjenu koja će se nacionalna pravila primjenjivati u dobi te osigurati odgovarajuće mehanizme za suglasnost roditelja, procese i provjere nad njima 3. Ukoliko se usluge nude izravno djetetu, potrebno ih je predstaviti obavijesti koje su jasno izrađene da ih dijete razumije	Prilikom nuđenja usluge Digitalne akademije, prikupljanja podataka putem web obrasca na http://digitalna-akademija.hr potrebno je definirati chebox : Imam više od 18 godina ili Prijavljujem svoje dijete Tehnička implementacija zahtjeva: - postavljanje zapisa za polja koja definiraju kategorije podataka koji se zaprimaju - uložiti napore kako bi se provjerilo odobrenje koje bi trebalo biti dano od strane nositelja roditeljske odgovornosti s dostupnom tehnologijom

	odgovornosti s dostupnom tehnologijom. To samo utječe na podatke na mreži-(online), dok oni izvanmrežni (offline*)* podaci će biti podložni uobičajenim pravilima države članice o sposobnosti za pristanak. Člankom 8. također je definirano kako navedeno ne utječe na opće ugovorno pravo država članica kao što su pravila o valjanosti, sklapanju ili učinku ugovora kada je riječ o djetetu. Organizacije moraju razmotriti lokalne zakone na ovom području.		

5.2.5. Osjetljivi podaci i zakonska obrada

Novi zahtjevi	Značajne promjene	Što je potrebno da bi se uskladili?	Usklađenost Algebra grupe
5. Osjetljivi podaci i zakonska obrada Agencija za zaštitu osobnih podataka kao mjerodavno tijelo u području nadzora nad zaštitom osobnih podataka sukladno članku 33. st. 1. podstavku 7. Uredbe o zaštiti osobnih podataka („Narodne novine“ broj 106/12 - pročišćeni tekst zakona) daje sljedeću preporuku za unapređenje zaštite u prikupljanju i daljnjoj obradi osobnih podataka korisnika usluga društva u navedene svrhe: - načelo razmjernosti nalaže kako je dozvoljeno prikupljati osobne podatke u opsegu koji je nužan za ispunjenje točno određene svrhe te se osobni podaci ne smiju prikupljati u većem opsegu nego što je nužno da bi se postigla zakonom utvrđena svrha. Zakonom o osobnoj	Da. Tehničke i organizacijske mjere: - ograničavanje pristupa nad podacima pohranjenim u zbirkama osobnih podataka – zaposlenicima voditelja zbirki s točno definiranom svrhom. Svrha je definirana procedura/ uputa prema kojoj zaposlenici obrađuju osobne podatke korisnika usluga društva (Algebra grupa) što je potrebno također definirati internim aktom s opisom uloga.	Osigurati interni akt te provesti ga kroz redizajnirane pravilnike unutar Društva. U svrhu poštene i zakonite obrade osobnih podataka sustavno, kontrolirano provoditi edukaciju osoba zaposlenih u obradi osobnih podataka. Pratiti službenika za zaštitu osobnih podataka prvenstveno u pogledu praćenja propisana iz područja zaštite osobnih podataka i primjene odgovarajućih mjera u zaštiti osobnih podataka. Osigurati postojanost zakonite svrhe i pravnog temelja.	U internom pravilniku Algebra grupe potrebno je revidirati tehničke i organizacijske mjere u kojima su propisane zakonite svrhe i pravni temelji za obradu osobnih podataka. Određeni osobni podaci moraju se prikupljati i čuvati prema definiranom roku od 2 godine do trajnog čuvanja. Također, potrebno je definirati ugovorne klauzule s izvršiteljima u ime Algebra grupe, njihove obveze i usklađenost s Uredbom. Za kopiranje osobne iskaznice postoji legitimni interes, nuđenje usluge koje vodi k sklapanju ugovora u kojem prema nacionalnom zakonodavnom tijelu se nalaže kopiranje

iskaznici („Narodne novine“ broj 62/15) kao posebno propisan zakon nalaže kako je osobna iskaznica elektronička javna isprava kojom hrvatski državljanin dokazuje identitet, hrvatsko državljanstvo, spol, datum rođenja i prebivalište u Republici Hrvatskoj. Sukladno tome, osobna iskaznica u svrhu nedvojbenog utvrđivanja identiteta ispitanika, te se time sprječava mogućnost zamjene identiteta i zlouporabu osobnih podataka.			osobne iskaznice s jasnom svrhom. Potrebno je izvršiti tehničku usklađenost gdje se čuvaju kopije osobnih iskaznica te potvrditi usklađenost kroz ograničenost uloga zaposlenika koji ostvaruju uvid u navedene osobne podatke kao i izvršiti procjenu i implementaciju usklađenosti tvrtki partnera koji predstavljaju izvršitelja obrade prema Algebri s obzirom na uslugu.

5.2.6. Obavijesti o privatnosti

Novi zahtjevi	Značajne promjene	Što je potrebno da bi se uskladili?	Usklađenost Algebra grupe
6. Obavijesti o privatnosti Voditelji obrade moraju preispitivati i ažurirati po potrebi kako bi se postigla i osigurala transparentnost obrade Također, navedene informacije moraju biti dostavljene, postoji opća obveza transparentnosti. Osigurati dodatne informacije – iako organizacijama može biti teško osigurati razdoblje osiguravanja. Naglasak se stavlja na jasnim, sažetim obavijestima.	Ne. Predstavlja ono što tvrtke trebaju imati, načelo „poštene“ i „transparentne“ obrade koje voditelj obrade mora dostaviti pojedincima o njegovoj obradi podataka. Također, voditelj obrade može također pružiti dodatne informacije ako je u posebnim okolnostima to neophodno u svrhu transparentne i pravedne obrade. Sve neophodne informacije trebaju biti dostavljene na transparentan, sažet, razumljiv i lako dostupan način.	Potrebno je uložiti napore u: 1. Pregledavanje dokumentacije postojećih obavijesti o privatnosti te ih ažurirati 2. Za podatke koji se prikupljaju neizravno provjeriti je li obavijest dana u odgovarajuće vrijeme, tj. web stranice.	Dokumentacija o politici zaštite osobnih podataka Algebra grupe podrazumijeva izmjenu i dopunu internog pravilnika o radu, redizajn ugovornih odnosa sa partnerima i dobavljačima, edukaciju zaposlenika i uska suradnja odjela prema ulogama unutar Algebra grupe. Također, preporučuje se objava politike zaštite privatnosti na web stranici Algebra grupe u vidu podizanja svjesnosti o zaštiti i povjerenja koje ispitanici daju kroz svoje osobne podatke. Dobro dizajnirane i lako dostupne nadzorne ploče omogućuju i pojedincima pristup kopijama svojih osobnih podataka, idealno u obliku koji se

			može ponovno upotrijebiti i koji je strojno čitljiv. Prijedlozi usklađivanja po ICO smjernica predstavljeni su u istom poglavlju, dijelu *Procjenu utjecaja na zaštitu podataka (DPIA).*

5.2.7. Pristup, ispravljanje i prenosivost podataka

Novi zahtjevi	Značajne promjene	Što je potrebno da bi se uskladili?	Usklađenost Algebra grupe
7. Pristup, ispravljanje i prenosivost podataka voditelj obrade mora na zahtjev: - potvrditi obrađuju li osobne podatke pojedinca; - osigurati kopiju podataka (u uobičajenom elektroničkom obliku u mnogim slučajevima); i - pružiti potporne (i detaljne) materijale U obradi osobnih podataka može se zahtijevati da se osobni podaci prenesu na njih ili na novog davatelja usluga u obliku u kojem se može čitati ako su podaci: 1. podložni voditelju obrade 2. obrađuju automatski 3. obrađeni na temelju suglasnosti ili ispunjenjem ugovora Zahtjev mora biti	Provjera obrade podataka ispitanika svrhom da je: - dobio uvid u osobne podatke pristup podacima te imati uvid u kopiju podataka (backup podataka) - osigurati dodatne informacije o obradama Nad svim obradama Voditelj mora poštivati djelovanje bez nepotrebnog kašnjenja i najkasnije u roku od mjesec dana, iako postoje mogućnosti produljenja roka. Voditelj obrade osobnih podataka mora koristiti razumne načine kako bi potvrdio identitet osobe koja je podnijela zahtjev, ali ne smije zadržavati ili prikupljati podatke	1. Pregledati procese organizacije, postupke te proći obuku s zaposlenicima 2. Razviti predloške odgovora kako bi se osiguralo da dokumentacija sadrži sve elemente, ujedno i sve prateće detaljne informacije 3. Mogu li se podaci stavljati u prijenosnom formatu (CSV itd.), te definirati mjere kojima će se zadovoljiti zahtjevi za pristup 4. Razmotriti odnose li se podaci na više od jednog nositelja podataka te definirati mjere	Svi zaposlenici su sudjelovali u identificiranju obrada osobnih podataka s obzirom na poslovnu aktivnost koju obnašaju u Algebra grupi. Kreirana je evidencija zbirki osobnih podataka, predložak odgovora na potencijalne upite i ostale prateće informacije. Pristup podacima definiran je ulogama (rolama u sustavu) u poslovnim aktivnostima Algebre u kojima voditelji odjela surađuju s Službenikom za zaštitu osobnih podataka u vidu praćenja usklađenosti u organizacijskim i tehničkim mjerama. Potrebno je definirati pristup podacima i u kojem obliku (formatu). Ukoliko se u različitim bazama pojavljuje ista osoba potrebno je izvršiti tehničku implementaciju

ispunjen u roku od jednog mjeseca (s produžetkom za neke slučajeve) i svaku namjeru ne pridržavanja mora se objasniti i specificirati pojedincu. Prava pristupa imaju za cilj dopustiti pojedincima da provjere zakonitost obrade i pravo na kopiju ne bi trebalo negativno utjecati na prava drugih.	samo kako bi mogla zadovoljiti osnovnu uslugu.	rješavanja poteškoća ovog oblika 5. Definiranje potrebe za razvoj pristupnih portala za pristup podacima s ciljem izravnog ostvarivanja prava pristupa 6. Osigurati usklađenost s vremenskim rokovima u ispunjavanju zahtjeva.	kroz uparivanje na postojeći profil ili kreiranje novog. Dokumentirati promjene kroz sustave. Predlaže se da ispitanicima bude dostupan uvid u osobne podatke putem mail linka na preglednu formu. Također, ukoliko ispitanik je dao telefonskim putem zahtjev, dostavlja mu se link na web adresu.

5.2.8. Pravo brisanja i ograničavanja obrade

Novi zahtjevi	Značajne promjene	Što je potrebno da bi se uskladili?	Usklađenost Algebra grupe
8. Pravo brisanja i ograničavanja obrade Pravo na zaborav (sada se nazivaju brisanjem) i pravo za ograničenje obrade. Pojedinci mogu zahtijevati da se podaci "brišu" kada postoji problem s zakonitosti obrade ili gdje ispitanik povlači pristanak za daljnje korištenje. Pojedinac može zahtijevati da voditelja obrade da se obrada „ograniči“ na obradu podataka dok se žalbe (na primjer, o točnosti) ne riješe ili ako je obrada nezakonita. Voditelji obrade koji su javno objavili podatke koja pripada pravu na brisanje po zahtjevima ispitanika, dužan je obavijestiti ostale koji obrađuju te podatke o pojedinostima zahtjeva.	Da.	1. Osigurati postupanje u skladu sa zahtjevima prava na brisanje podatka 2. Uskladiti sustave da su u stanju ispuniti zahtjeve za označavanje podataka kao *ograničene* dok ispitanik prolazi proces žalbe ili ostvaruje potrebu za brisanje podataka.	U marketinške svrhe privole su predstavljene i opisane s obzirom na svrhu te je ponuđen korisniku odabir komunikacijskog kanala putem kojeg želi ostvarivati komunikaciju s nama. Sustavi Algebre usklađeni su s pravom ispitanika na prava koja ostvaruje ukoliko žele izjasnit svoje mišljenje o dijeljenju svojih osobnih podataka u svrhe koja mu je jasno, nedvosmisleno predočena. Ukoliko Algebra grupa nema legitimni interes za čuvanje osobnog podataka, ispitanik ostvaruje prava prema Uredbi. Tehnička implementacija vrši se automatiziranim putem kroz CRM sustav, dok Službenik za zaštitu osobnih podataka također ima obveze u ovom području.

5.2.9. Pravo na prigovor

Novi zahtjevi	Značajne promjene	Što je potrebno da bi se uskladili?	Usklađenost Algebra grupe
9. Pravo na prigovor Pojedinac prema Uredbi ima definirana prava da se protivi određenim vrstama obrade osim onih čija je: - obrada temeljena na legitimnom interesu, obavljanju zadaće u javnom interesu/ obavljanju službenih ovlasti - obradi u istraživačke ili statističke svrhe Prema Uredbi, pojedinac ostvaruje pravo prigovora samo na direktni marketing, odnosno za navedeno ne treba dokazati osnovu za prigovor. Obveze ponuditelja usluge jest da pojedince (ispitanike)	Ne.	1. Revidirati politike kako bi se osiguralo da se pojedincima omogući prava na prigovor, jasno i zasebno, na mjestu „prve komunikacije“ 2. Provjeriti područje mrežnih usluga, postoji li automatska detekcija za s obzirom na prava ispitanika 3. Pregledati procese i propise pružatelja usluga organizacijama (partneri i davatelja usluga) kako bi se provjerila usklađenost.	Pravo na prigovor koje prema Uredbi ispitanik ostvaruje, Algebra grupa implementirala je u svoje poslovanje i prilagodila se zahtjevima koje Uredba nalaže. Pravo na prigovor korisnici trenutno mogu ostvariti mailom, osobnim dolaskom ili poštom. Preporučuje se da klijenti upućuju administriranje online forme ili upućivanjem prigovora putem online forme za prigovor Implementacija zahtjeva tehničke mjere usklađivanja sa sustavima. Predlaže se da prigovor kreira *ticke*t u CRM-u koji se potom obrađuje. Obrada je manulana, u izvornim sistemima. Pružatelji usluga, partneri, dobavljači tvrtke su koje su svoju usklađenost također provele nad svojim organizacijama, te je prema njima, izvršiteljima obrade dodana klauzula u ugovornom odnosu kojim se pružatelj usluga obvezuje uskladiti svoje poslovanje s Uredbom.

obavijesti o pravima u ranoj fazi, jasno i zasebno od drugih informacija. Online usluge moraju ponuditi automatsku metodu prigovora.			

5.2.10. Obveze organizacijske usklađenosti

Novi zahtjevi	Značajne promjene	Što je potrebno da bi se uskladili?	Usklađenost Algebra grupe
10. Obveze organizacijske usklađenosti Uredba nalaže da organizacije provedu široki spektar mjera u svrhu smanjenja rizika od kršenja i dokazivanje ozbiljnosti u načinu upravljanja osobnim podacima. Te mjere uključuju: procjenu utjecaja na privatnost, revizije, politike organizacije, evidencije aktivnosti obrada i imenovanje Službenika za zaštitu osobnih podataka (DPO). Ukoliko se organizacije ne usklade prijeti im visoka novčana kazna za nepoštivanje Uredbe.	Da.	1. Definiranje odgovornosti i proračuna za usklađivanje 2. Imenovanje DPO i njegove autonomnosti u skladu s drugim radnim opterećenjem i poslovnim procesima unutar organizacije 3. Nadzorno tijelo očekuje suradnju s odborom/upravom organizacija te specificiranje aktivnosti zaposlenika koji usko surađuju s DPO-om 4. Zadaća DPO-a je osigurati kompletnu usklađenost koje uključuje značajke poput: procjena utjecaja na privatnost (DPIA), regularne DP audite, preglede politika i ažuriranja te edukacija zaposlenih i podizanje svijesti unutar organizacije 5. Revidiranje pravila i uvjeta dobavljača,	Algebra grupa u procesu je revidiranja internih pravilnika politike zaštite osobnih podataka. Sukladno usklađivanju, potrebno je na vrijeme održati interni audit o zaštiti osobnih podataka i obradama nad njima. Inicijalni interni sastanak uključuje: - Upravu Algebra grupe - Službenika za zaštitu osobnih podataka - voditelje odjela - tehničku podrška Službenik za zaštitu osobnih podataka (DPO) interni je voditelj upućen u poslovne aktivnosti poslovnih aktivnosti Algebra grupe. Usko surađuje s voditeljima odjela u obradi nad osobnim podacima ovisno o svrsi. Surađuje s nadzornim tijelom u vidu aktivnosti kada je to zakonom propisano. Predstavljena je preporuka DPIA preko koje je definirana dokumentacija s

		partnera u obradi osobnih podataka.	obzirom na procijenjeni rizik obrada i usklađenosti s obradama. Službenik za zaštitu osobnih podataka predlaže sljedeći audit u svrhu kontrole nad obradama ispitanika. Ažuriranje s dokumentacijom sukladno Uredbi i nacionalnim zakonima, edukacija zaposlenih u mjeri potrebnoj za postupanjem s osobnim podacima, nova klauzula u ugovornim odnosima, obveze izvršitelja i Algebra grupe postignut je konsenzus nad Uredbom prema tehničkim i organizacijskim implementacijskim mjerama. Zaposlenici Algebra grupe upoznati su s evidencijom koja se vodi nad njima u vidu osobnih podataka za koje Algebra grupa ostvaruje legitimni interes. Upoznati su s vrstom osobnih podataka i u koje svrhe se obrađuju te potvrđuju legtimitet obrade. Čuvaju se u definiranom roku od 2 god do onih trajnog roka čuvanja. Tehnički su poduzete mjere sigurnosne zaštite nad njima, kao i ograničeni uvidi zaposlenika u navedeno.

5.2.11. Privacy by design

Novi zahtjevi	Značajne promjene	Što je potrebno da bi se uskladili?	Usklađenost Algebra grupe
11. Privacy by design Pristup projektima koji služi za usklađivanje privatnosti i sukladnosti zaštite podataka unutar organizacija sa zakonskim obvezama, pomaže pri mininimiziranju rizika privatnosti i izgradnju povjerenja.	Da. Organizacije moraju provoditi tehničke i organizacijske mjere kako bi dokazale da su svoje mjere aktivnosti obrade podataka integrirale u poslovne procese.	Odgovarajuće role (definiranje uloga) nad osobnim podacima i uporaba pseudonimizacije ili enkripcije nad podacima. Predlaže se izrada i ažuriranje procedure za obavještavanje o internim prekršajimaincidentima, uključujući procese identifikacije incidenta (IT sustavi) i planove djelovanja na incidente.	Uspostavljene su sigurnosne tehničke mjere IT sustava Algebra grupe. Minimizirani su podaci koji se prikupljaju i definirani svrhom prikupljanja s obzirom na legitimne interese koje ostvaruje Potrebno je definirati rok provjere i testiranja sustava s ciljem sprječavanja zlouporabe osobnih podataka.

5.2.12. Povreda osobnih podataka

Novi zahtjevi	Značajne promjene	Što je potrebno da bi se uskladili?	Usklađenost Algebra grupe
12. Povreda osobnih podataka Prema članku 4. stavka definicije povreda osobnih podataka predstavlja: *„povreda osobnih podataka" znači kršenje sigurnosti koje dovodi do slučajnog ili nezakonitog uništenja, gubitka, izmjene, neovlaštenog otkrivanja ili pristupa osobnim podacima koji su preneseni, pohranjeni ili na drugi način obrađivani."*	U roku od 72 sata od kršenja Uredbe potrebno je obavijestiti nadzorno tijelo u skladu sa zahtjevima Izuzeće predstavlja: - Rješenje vjerojatno neće rezultirati visokim rizikom za prava i slobode pojedinaca - Odgovarajuće tehničke i organizacijske zaštite bile su aktivne u vrijeme incidenta (šifrirani podaci)	Izraditi i ažurirati procedure za obavještavanje o internim prekršajima /incidentima, uključujući procese identifikacije incidenta i planove djelovanja na incidente te ih provesti kroz IT sustave.	Službenik za zaštitu osobnih podataka predstavio je na auditu procedure za obavještavanje o internim prekršajima/incidentima te planove djelovanja nad ponovnu zaštitu. Aktivno se prate organizacijski i tehnički aspekti poslovanja u skladu sa zahtjevima o zaštiti osobnih podataka i drugih nacionalnih pravnih akta Republike Hrvatske.

5.2.13. Transfer osobnih podataka

Novi zahtjevi	Značajne promjene	Što je potrebno da bi se uskladili?	Usklađenost Algebra grupe
13.Transfer osobnih podataka Prijenos osobnih podataka primateljima u "trećim zemljama" (tj. Izvan Europskog ekonomskog područja (EEA)) i dalje se regulira i ograničava u određenim okolnostima. Treća zemlja trebala bi ponuditi jamstva kojima osigurava primjerenu razinu zaštite podataka. Nadalje, navodi se kako je prema članku 46. stavka 1 (c) : "*prijenos je nužan radi sklapanja ili izvršavanja ugovora sklopljenog u interesu ispitanika između voditelja obrade i druge fizičke ili pravne osobe."*	Ne.	1. Pregled ključnih međunarodnih tokova podataka (info revizija) 2. Revidiranje standardnih predložaka u nabavi i klauzule ugovora s obzirom na vašu odgovornost prema dobavljačima.	Osobni podaci koje Algebra prikuplja u skladu su s propisima koje Uredba nalaže, a transfer tih istih podataka prenosi primatelju po zakonu definiranom prema "trećim zemljama".

Tablica 6. Gap analiza Algebra grupe

Izvor: Autorov rad prema Gloucestershire Care Services (NHS Trust)

5.3 Pravna podloga za provođenje obrada sukladno: Zakonima, Ugovornim odnosima i Privolama – prikaz evidencije obrade sukladno navedenom

Sukladno brojnim zakonskim aktima prema nadležnom tijelu u obrazovnom sustavu, Agenciji za znanost i visoko obrazovanje (AZVO) Republike Hrvatske prema kojima Algebra grupa provodi usklađenost prema standardima i kvalifikacijama agencije. Agencija za znanost i visoko obrazovanje djeluje samostalno i neovisno u djelokrugu i nadležnosti utvrđenih Zakonom o znanstvenoj djelatnosti i visokom obrazovanju i Zakonu o priznavanju inozemnih obrazovnih kvalifikacija. Javni interes u očuvanju standarda visokoobrazovnih kvalifikacija misija je Agencije za znanost i visoko obrazovanje, koja u vidu misije usko surađuje s visokoobrazovanim ustanovama, znanstvenim organizacijama, Nacionalnim vijećem za znanost, Nacionalnim vijećem za visoko obrazovanje, Ministarstvo znanosti, obrazovanja i športa te ostalim državnim tijelima u području visokog obrazovanja i znanosti.

Nadalje, Algebra grupa također posluje prema *Zakonu o zaštiti na radu* (NN broj 71/14) prema kojem provodi usklađenost u sprječavanju nastanka požara i eksplozije. U tom području prikuplja osobne podatke koji su nužni za svrhu i ostvaruje legitimni interes. Osobni podaci prikupljeni su elektronskim oblikom, a kategorije osoba od kojih se prikupljaju osobni podaci su zaposlenici, a sami podaci koji se prikupljaju su:

- ime i prezime
- OIB
- datum rođenja
- adresa i mjesto stanovanja
- obrazovanje
- stupanj obrazovanja
- naziv radnog mjesta

Pristup nad podacima ima Odjel operacija, Zaštita na radu i zaštita od požara. Isti podaci ne prosljeđuju se i čuvaju se trajno sa tehničkim mjerama s kojima se usklađuje sa zahtjevima GDPR-a.

Također, prema Zakonu o radu predstavljene su sljedeće aktivnosti i podaci koje Algebra grupa provodi i obrađuje sukladno Zakonu o radu.

Poslovna aktivnost	Odjel	Način spremanja	Kategorija osoba	Kategorija podataka	Podaci
Evidencija zaposlenika	ljudski potencijali	elektronski	zaposlenici	biografski podaci/kontakt podaci/kvalifikacije/vještine/ administrativni podaci (OIB..)	podaci nužni za svakodnevno poslovanje
Ugovori o radu/ suradnji	ljudski potencijali	elektronski	zaposlenici	biografski podaci/kontakt podaci/administrativni podaci (npr. OIB)/podaci o plaći/podaci o tipu zapošljavanja	podaci nužni za svakodnevno poslovanje
Dosjei zaposlenika	ljudski potencijali	papirnati	zaposlenici	biografski podaci/kontakt podaci/administrativni podaci (npr. OIB)/podaci o plaći/podaci o tipu zapošljavanja	podaci nužni za svakodnevno poslovanje

Poslovna aktivnost	Točke prikupljanja podataka	Tko ima pristup	Kome se prosljeđuju podaci- samo unutar poduzeća	Period čuvanja	Period ažuriranja
Evidencija zaposlenika	e-mailom ili osobnim kontaktom	Odjel upravljanja ljudskim potencijalima i računovodstva	Uprava, voditelji (svaki za svoje zaposlenike), odjel računovodstva	trajno	povremeno
Ugovori o radu/ suradnji	e-mailom ili osobnim kontaktom	Odjel upravljanja ljudskim potencijalima , uprava i računovodstva	Odjel računovodstvo	trajno	povremeno
Dosjei zaposlenika	e-mailom ili osobnim kontaktom	Voditeljica upravljanja ljudskim potencijalima, računovodstvo	Odjel računovodstvo	trajno	povremeno

Tablica 7. Obrada podataka Algebra grupe sukladno Zakonu o radu

Izvor: Vlastiti rad

Podaci koji se prikupljaju ugovorom o radu:

Ime/prezime/adresa/poštanski broj/mjesto/država/OIB/naziv radnog mjesta i opis radnog mjesta/tip zapošljavanja/iznos plaće u bruto 1 iznosu + iznos prijevoza

Podaci koji se prikupljaju za interni dosje zaposlenika:
Ime/prezime/adresa/poštanski broj/mjesto/država/OIB/naziv radnog mjesta i opis radnog mjesta/tip zapošljavanja/iznos plaće u bruto 1 iznosu + iznos prijevoza/ dokumentacija (rodni list, izjava o nekažnjavanju, kopija osobne iskaznice i tekućeg računa, domovnica, porezni karton)

Podaci koji se prikupljaju u svrhu evidentiranja zaposlenika su:

Ime/prezime/ime oca/adresa/poštanski broj/mjesto/država/mjesto rođenja/e-mail/telefon/stručna sprema/godine radnog iskustva/spol/datum rođenja/staž/staž u Algebri/datum zapošljavanja u Algebri/akademski stupanj/titula/JMBG/OIB/državljanstvo/struka/završena srednja škola/završen fakultet/radno mjesto/odjel/vrsta ugovora o radu/tip zapošljavanja/otkaz/tip otkaza/smjenski rad/voditeljska-nevoditeljska radna uloga/osobni odbitak/iznos bruto plaće/iznos neto plaće/korištenje benefita

Zakonom o arhivskoj građi Algebra grupa obvezuje se na čuvanje, uporabu i obradu arhivskog gradiva. Sukladno zakonom prikuplja osobne podatke predstavljene u tablici ispod.

Poslovna aktivnost	**Odjel**	**Način spremanja**	**Kategorija osoba**	**Kategorija podataka**	**Podaci**	**Točke prikupljanja podataka**
Rezultati ispita	Odjel operacija	Papirnato/ digitalno	klijenti/polaznici /studenti	osnovni osobni podaci, ishod ispita, rezultati vježbi	ime i prezime, rezultat ispita, bodovi	Pisano od kandidata, osobno od studenata putem maila

Tko ima pristup	**Kome se prosljeđuju podaci- samo unutar poduzeća**	**Period čuvanja**	**Period ažuriranja**
Svi koji imaju ključ od učionica, voditelj katedre za operacijske sustave, odjel za podršku nastavi i asistenti na katedri	Ne prosljeđuju se	Rezultati ispita čuvaju se u papirnatom obliku 2 godine, dok se u digitalnom obliku čuvaju trajno	Ne ažurira se

Tablica 8. Obrada podataka Algebra grupe sukladno Zakonu o arhivskoj građi

Izvor: Vlastiti rad prema evidenciji obrade Algebra grupe

Podaci u papirnatom obliku spremaju se u definiranom prostoru Algebra grupe, dok se oni u digitalnom obliku spremaju u integraciji s CRM sustavom kojeg koriste u svakodnevnom poslovanju.

Predstavljene obrade sukladne su zahtjevima zakonskih akta koje također moraju biti usklađene s zahtjevima o obradi osobnih podataka. U nastavku, prema podacima u tablicama predstavljene su preporuke organizacijskih i tehničkih mjera s naglaskom na odjel marketinga.

5.4 Izvršenje programa usklađenosti poslovnih procesa u organizacijsku strukturu Algebra grupe s naglaskom na odjel marketinga

Tehnološki napredak i dostignuća utjecala su na promjenu u načinu oglašavanja proizvoda i usluga. Tako je pojam internetski marketing ili digitalni marketing svojevrsno promijenio način oglašavanja te danas predstavlja ključan faktor uspješnih *online* kampanja. Za razliku od konvencionalnog pristupa donosi mogućnost preciznijeg ciljanja željenih skupina, ima daleko nižu cijenu ulaganja te omogućuje mjerljivost povrata na investiciju (ROI). Nadalje, u odnosu na tradicionalni marketing u svakom trenutku moguće je provjeriti isplativost investicije oglašavanja te je moguće na vrijeme zaustaviti kampanju koja ne ostvaruje zadovoljavajući povrat. Možemo reći da digitalni marketing predstavlja trenutno najučinkovitiji oblik oglašavanja u svijetu. S obzirom na mogućnost mjerenja uspješnosti kampanja bilo putem oglasa ili preko društvenih mreža uz pomoć digitalnih alata postavlja se pitanje što zapravo mjerimo u digitalnom marketingu? Digitalni alati tvrtkama i oglašivačima omogućuju da prate ponašanje posjetitelja web stranica putem *Cookies-a* te im omogućuje plasiranje ciljanih oglasa. Također, digitalni marketinški proces uključuje prikupljanje kontakata i generiranje *leadova,* čuvanje podataka o kontaktima i njihovo korištenje u daljnje svrhe te zadržavanje i dijeljenje podataka trećim stranama. Upravo iz tog razloga javila se potreba za ograničavanjem korištenja osobnih podataka bez pristanka ciljane osobe. Cilj nadolazeće Uredbe, predstavlja usklađivanje zakona svih država članica EU s ciljem razumijevanja pojedinca kako se koriste njihovi osobni podaci i u koje svrhe. Drugim riječima, Uredba se donosi kako bi se osigurala transparentnost između tvrtki koje prikupljaju i upravljaju podacima te korisnika koji su svoje podatke dali tvrtkama na korištenje i daljnje aktivnosti. U nastavku predstavit će se cjelokupna bit uredbe u odnosu na digitalni marketing te promjene koje sva poduzeća moraju implementirati u svoje marketinško poslovanje.

Pristanak

Kako bi tvrtke bile usklađene sa zahtjevima Uredbe, sva poduzeća moraju jasno i nedvosmisleno navesti kako i u koje svrhe koriste osobne podatke te omogućiti jasan i nedvosmislen pristanak za korištenje osobnih podataka koje će se smatrati ujedno i odobrenjem pojedinaca. Više neće biti dovoljno da posjetitelji kliknu *„Slažem se“* prilikom prihvaćanja usluge za koju su se registrirali ili za uslugu u kojoj prilikom posjećivanja web stranice servisa pristaju na uporabu *cookiesa*. Ova promjena svakako će unazaditi analitiku posjetitelja u vidu drastičnijeg broja posjeta weba, no UX dizajneri morati će biti kreativniji prilikom korisničkog iskustva kako bi posjetitelji što lakše surfali webom.

E-mail marketing kampanje

Prema Uredbi, e-mail marketing kampanje također podrazumijevaju usklađivanje. Od tvrtki, prilikom marketinške kampanje mailom zahtijeva se prikupljanje dobrovoljne, posebne, informirane i nedvosmislene privole. Privola kao takva mora obuhvatiti *„sve aktivnosti obrade koje se obavljaju u istu svrhu ili svrhe“*. Ukoliko obrada osobnih podataka ima višestruke svrhe, potrebno je dati privole za svaku od njih. Kako bi tvrtke postigle sukladnost potrebno je usvojiti nove prakse poput:

- nova vrsta opt-in s preporukom na korištenje double opt-in
- dokazati postojanost privola u sustavu
- usvajanje metode pravo na brisanje iz sustava

Tvrtke će trebati više vremena za sakupljanje kontakata, informacija i karakteristike o korisnicima. Postoji mogućnost da će se u kratkom roku sakupiti manje kontakata nego što je bilo do sada, no ti kontakti će biti vrjedniji u mailing listi što dovodi do ostvarivanja kvalitetnijih kampanja, bolji KPI-evi..

Newsletter

Newsletter kampanje također podliježu Uredbi o zaštiti nad osobnim podacima. Tvrtke će trebati tražiti pristanak primatelja newslettera jer uredba zabranjuje slanje mailove s ponudama tvrtke bez da ih se implicitno pita. E-mail se, prema uredbi smatra osobnim podatkom te ukoliko se u bazi podataka nalazi zapis ime.prezime@gmail.com osoba vam treba dati privolu da joj pošaljete e-mail.

Prijedlozi usklađivanja newsletter kampanje

- ne kupujte baze e-mailova
- kreirajte *double opt-in* opciju (postojećim bazama korisnika pošaljite novi email u kojem će te dobiti privolu i potvrdu)
- prijavite bazu primatelja newslettera Agenciji za zaštitu osobnih podataka (AZOP)
- gdje god se baza nalazila, podaci unutar nje trebaju biti zaštićeni imenom i lozinkom
- ukoliko se na web stranici tvrtke nalazi opcija u kojoj korisnici ostavljaju svoj e-mail kako bi preuzeli PDF dokument ne smijete im slati newsletter ukoliko nemate privolu za tu aktivnost

5.5 Ispunjavanje prava ispitanika

Načelno, nad ostalim podacima koji se obrađuju a nemaju pravni temelj poput zakonskih akta zahtijeva prikupljanje podataka na temelju privola ispitanika. Minimizacija osobnih podataka u načelu podrazumijeva da se prikupljeni i obrađivani podaci svedu na minimum potrebnih osobnih podataka koji su potrebni organizaciji sa ostvari definiranu svrhu. Kod primjerice zaposlenika, preko Pravilnika unutar poduzeća i drugim povezanim aktima postoji legitimni interesi za navedenu obradu. No, kada su osobni podaci prikupljeni s internet stranice putem kontakt forme, potrebno je minimizirati tražene osobne podatke kako bi mogli ostvariti navedenu svrhu. Algebra grupa prikuplja osobne podatke putem web obrasca u marketinške i prodajne svrhe te u svrhe profiliranja korisnika. U nastavku opisan je postupak prema kojem se organizacija mora uskladiti kada su u pitanju privole ispitanika.

Zakon o zaštiti osobnih podataka definira skup prava koja ispitanik ostvaruje, a zadaća voditelja obrade, koji posjeduje osobne podatke jest da omogući ispitaniku, u pravilu roka od mjesec dana da ostvari svoja prava. Prema tome, ispitaniku se mora omogućiti da ostvari sva prava koja prema Uredbi ima, osim ako pravna regulativa hrvatskih zakona ne dozvoljava da korisnik može ostvariti to pravo. Zakon o mirovinskom osiguranju i Zakon o zdravstvenom osiguranju nalaže prilikom obračuna plaća da se osobni podaci drže trajno, čak i kada zaposlenik više nije u poslovnom odnosu s poduzećem, pa čak i do 50 godina nakon što je prestao raditi za poduzeće. Upravo iz navedenog, ispitanik ne može ostvariti pravo na brisanje podataka.

Osnovna prava ispitanika

Prilikom davanja svojih osobnih podataka voditelju zbirke osobnih podataka građanin mora biti svjestan prava koja ostvaruje prema uredbi, odnosno treba biti upućen u koje točne svrhe daje svoje podatke. Tako, prema uredbi ispitanik ostvaruje sljedeća prava:

1. Pravo na pristup
2. Pravo na ispravak
3. Pravo na brisanje
4. Pravo na ograničavanje obrade
5. Pravo na prijenos podataka
6. Pravo na prigovor

U nastavku su predstavljena prava koja ispitanik ostvaruje:

1. Pravo na pristup

Pravo na pristup uključuje pravo od strane ispitanika da zna tko raspolaže podacima, odnosno pravo po kojem ispitanik ima pravo zatražiti od organizacije, pravne ili fizičke osobe koja raspolaže osobnim podacima uvid u osobne podatke koji se čuvaju u nekoj od zbirki osobnih podataka. Prema članku 15. stavka 1 navodi prava ispitanika na pristup osobnim podacima i sljedećim informacijama:

a) Svrsi obrade
b) Kategorijama osobnih podataka
c) Primateljima ili kategorijama primatelja kojima su osobni podaci otkriveni ili će im biti otkriveni, osobito primateljima u trećim zemljama ili međunarodnim organizacijama
d) Predviđeno razdoblje u kojem će osobni podaci biti pohranjeni, ili kriteriji korišteni za utvrđivanje razdoblja
e) Postojanje prava da se od voditelja obrade zatraži ispravak ili brisanje osobnih podataka ili ograničavanje obrade koji se odnose na ispitanika ili prava na prigovor na takvu obradu
f) Pravo na podnošenje pritužbe nadzornom tijelu
g) Ukoliko se podaci ne prikupljaju od ispitanika, svakoj dostupnoj informaciji o njihovom izvoru
h) Automatizirano donošenje odluka, što uključuje izradu profila [19]

2. Pravo na ispravak

Prema pravu na ispravak, ispitanik ima pravo zatražiti od voditelja obrade ispravak netočnih osobnih podataka koji se odnose na njega.

3. Pravo na brisanje („pravo na zaborav“)

Prema pravu na brisanje ispitanik ima pravo od voditelja obrade zatražiti brisanje osobnih podataka bez nepotrebnog odgađanja ukoliko je ispunjen jedan od sljedećih uvjeta po članku 17. stavka 1.:

a) *Osobni podaci koji nisu više nužni u odnosu na svrhu za koju su prikupljani ili na drugi način obrađivani*
b) *Ispitanik ima pravo povući privolu na kojoj se obrada temelji*
c) *Ispitanik uloži prigovor na obradu u skladu s obradom koja je nužna za izvršavanje zadaće od javnog interesa ili pri izvršavanju službene ovlasti voditelja obrade te kada je obrada nužna za potrebe legitimnih interesa voditelja obrade ili treće strane te kada su od tih interesa jači interesi ili temeljna prava i slobode ispitanika koji zahtijevaju zaštitu osobnih podataka, osobito ako je ispitanik dijete*
d) *Osobni podaci nezakonito su obrađeni*
e) *Osobni podaci moraju se brisati radi poštovanja pravne obveze iz prava Unije ili prava države članice kojem podliježe voditelj obrade*
f) *Osobni podaci prikupljeni su u vezi s ponudom usluga informacijskog društva prema kojem u pogledu nuđenja usluga informacijskog društva, obrada je zakonita samo ako dijete ima najmanje 16 godina i u mjeri u kojoj je privola dana ili odobrena od nositelja roditeljske odgovornosti nad djetetom* [20]

Također, ukoliko je voditelj obrade objavio javne podatke dužan je u skladu s navedenom stavkom 1 istog članka, obrisati te osobne podatke, uzimajući u obzir dostupnu tehnologiju i trošak provedbe. (stavka 2.)

Navedene stavke 1 i 2 ne primjenjuju se u mjeri u kojoj je obrada nužna:

a) *Radi ostvarivanja prava na slobodu izražavanja i informiranja*
b) *Radi poštovanja pravne obveze kojom se zahtijeva obrada u pravu Unije ili pravu države članice kojem podliježu voditelj obrade ili za izvršavanje zadaće od javnog interesa ili pri izvršavanju službene ovlasti voditelja obrade.*
c) *Radi javnog interesa u području zdravlja*
d) *U svrhe arhiviranja u javnom interesu, znanstvenog ili povijesnog istraživanja ili u statističke svrhe*
e) *Radi postavljanja, ostvarivanja ili obrane pravnih zahtjeva* [21]

4. Pravo na ograničavanje obrade

Prema pravu na ograničavanje obrade ispitanik ima pravo od voditelja obrade ishoditi ograničenje obrade ukoliko je ispunjeno jedno od sljedećeg:

a) *Ispitanik osporava točnost osobnih podataka, na razdoblje kojim se voditelju obrade omogućuje provjera točnosti osobnih podataka*
b) *Obrada je nezakonita i ispitanik se protivi brisanju osobnih podataka te umjesto brisanja traži ograničenje uporabe*
c) *Voditelj obrade više ne treba osobne podatke za potrebe obrade, ali ih ispitanik traži radi postavljanja, ostvarivanja ili obrane pravnih zahtjeva*
d) *Ispitanik je uložio prigovor na obradu osobnih podataka očekujući potvrdu nadilaze li legitimni razlozi voditelja obrade razloge ispitanika* [22]

Ukoliko je obrada ograničena navedenim stavkama osobni podaci smiju se obrađivati samo ukoliko postoji privola ispitanika, uz iznimku pohrane ili za postavljanje ili obranu pravnih zahtjeva ili zaštitu prava druge fizičke ili pravne osobe ili zbog važnog javnog interesa Unije ili države članice.

5. Pravo na prenosivost podataka

Ispitanik ima pravo zaprimiti podatke koji se odnose na njega, koje je pružio voditelju obrade u strukturiranom, uobičajeno upotrebljavanom i strojno čitljivom formatu, te ostvaruje pravo prenosivosti drugom voditelju ukoliko se:

a) *Obrada temelji na privoli u jednu ili više posebnih svrha te ukoliko je ona nužna za izvršavanje ugovora u kojem je ispitanik stranka ili kako bi se poduzele radnje na zahtjev ispitanika prije sklapanja ugovora.*
b) *Obrada provodi automatiziranim putem* [23]

6. Pravo na prigovor

Ispitanik ima pravo na temelju svoje posebne situacije u svakom trenutku uložiti prigovor na obradu osobnih podataka koji se odnose na njega. Načelno, voditelj obrade ne smije više obrađivati osobne podatke ukoliko ne dokaže da postoje uvjerljivi legitimni razlozi za obradu koji nadilaze interese, prava i slobode ispitanika ili u slučaju pravnih zahtjeva. Nadalje, ukoliko se ti osobni podaci obrađuju u svrhu izravnog marketinga, ispitanik u svakom trenutku ima pravo uložiti pravo na prigovor, što uključuje izradu profila u mjeri koja je povezana s takvim izravnim marketingom.

S obzirom na marketinšku svrhu za navedene obrade koja odrađuje partner tvrtka potrebno je zahtijevati privolu od ispitanika, stoga su u sljedećem dijelu predstavljeni glavni elementi Algebra grupe prilikom kreiranja privole za marketinške svrhe.

Preporuka informacija (*draft*) koje treba sadržavati privola:

Vaše podatke Algebra grupa u ime subjekata Visoko učilište Algebra, Pučko otvoreno učilište i Algebra d.o.o obrađuje sukladno relevantnim odredbama Uredbe, stoga je ova potvrda dana je slobodno i neuvjetovano. Također, zadržavate pravo opozivanja privole u svakom trenutku. Ukoliko vaše osobne podatke planiramo obrađivati u svrhe koje nisu ovdje opisane ili se nalaze izvan svrhe za koju ste pružili privolu, prije takve obrade nadređena osoba pružiti će vam informacije o drugoj svrsi i sve ostale relevantne informacije o obradi.

Ukoliko želite primati novosti Algebra grupe o proizvodima, uslugama i eventima, pribilježite se i ostvarite kontakt s nama. Prikupljamo osobne podatke sukladno poslovnoj aktivnosti:

Prikupljamo osobne podatke sukladno poslovnoj aktivnosti:

Marketinška aktivnost:

U svrhu poslovne aktivnosti marketinga, podatke koje obrađujemo temeljene su na legitimnom interesu izvršenje ugovornih obveza s ispitanikom. Vaši osobni podaci koje prikupljamo u svojem poslovanju u potpunosti su sigurni.

Saznajte <u>više</u> o obradi osobnih podataka

Prodajna aktivnost

U svrhu poslovne aktivnosti prodaje, podatke koje obrađujemo temeljene su na legitimnom interesu izvršenje ugovornih obveza s ispitanikom. Vaši osobni podaci koje prikupljamo u svojem poslovanju u potpunosti su sigurni.

Saznajte <u>više</u> o obradi osobnih podataka

Profiliranje

Pored podataka nad kojima nam dajete pristup, vaši osobni podaci biti će pohranjeni kod treće strane MailChimp newsletter platforme koju koristimo prilikom marketinške komunikacije s Vama. Pristup tim podacima i pravo korištenja ima samo naša strana.

Saznajte više o obradi osobnih podataka

Slažem se s uvjetima i odredbama.

☐ *Imam više od 18 godina*

Pod više:

(Odjel marketinških komunikacija i Odjel prodaje koristi vaš e-mail, ime i prezime te adresu prilikom prijave _____ za koje ste se prijavili putem naše web forme.

Odvojenu privolu dajete nam za slanje promotivnih ponuda na vaš e-mail. Obrađuju se podaci poput ip-adrese i cookie, koji se koristi kratkoročno u svrhu poboljšanja korisničkog iskustva.

Vaše podatke ne dijelimo van okvira potrebe za izvršavanjem osnovne usluge.

Podatke koje dijelimo s partnerima:

- *MailChimp*
- *Infomar d.o.o*

Vaše povjerenje nam je dragocjeno, vaši osobni podaci kod nas su sigurni, ne dijele se, ne prodaju ili ustupaju drugim privatnim ili pravnim osobama na druge namjene osim onih za koje je navedena svrha.

Podatke čuvamo

Sve potrebne podatke za pružanje usluga koje ste dali pri registraciji na našoj stranici ni na koji način ne prikuplja, kupuje, nabavlja vaše osobne podatke od trećih osoba.

Također, možete zatražiti da uklonimo Vaše podatke ili povući privolu za korištenje. Pošaljite nam email na adresu dpo@algebra.hr kako bismo pokrenuli proceduru prema pravu na brisanje. S povratnom informacijom obavijestiti ćemo Vas u roku od 15 dana.

Privolu za slanje newslettera možete povući samostalno, u postavkama na svom profilu.

U svakom trenutku možete dobiti uvid svih svojih podataka putem linka _____ .)

Na temelju okvirnog sadržaja privole, predstavljen je obrazac za prihvaćanje suglasnosti za obradu osobnih podataka Algebra grupe:

Davanjem ove privole i ustupanjem Vaših osobnih podataka unosom u ovaj prijavni obrazac pristajete na obradu niže navedenih vrsta osobnih podataka u svrhu koju označite u ovom obrascu. Opširnije o davanju privole i načinu upravljanja Vašim osobnim podacima možete pročitati ovdje.

*Podatke koje navedete u ovom obrascu koristit ćemo isključivo u sljedeću svrhu (**molimo označite kvačicom**):*

- marketinške svrhe - dostavljanje informacija, ponuda i promidžbenih materijala o proizvodima ili uslugama Algebra grupe

Za navedenu svrhu obrade, pristajem da me članice Algebra grupe kontaktiraju putem sljedećih komunikacijskih kanala (molimo odaberite):

- Emailom na niže navedenu email adresu
- Telefonskim pozivom na niže navedeni broj fiksnog telefona
- Telefonskim pozivom na niže navedeni broj mobilnog telefona
- Telefonskom porukom (SMS, WhatsApp, Viber ili slično) na gore navedeni broj mobilnog telefona
- Dostavom promotivnih materijala na kućnu adresu

Vaši osobni podaci:

Ime: Prezime:

Email adresa: Broj fiksnog telefona:

Broj mobilnog telefona:

Kućna adresa ili adresa ureda:

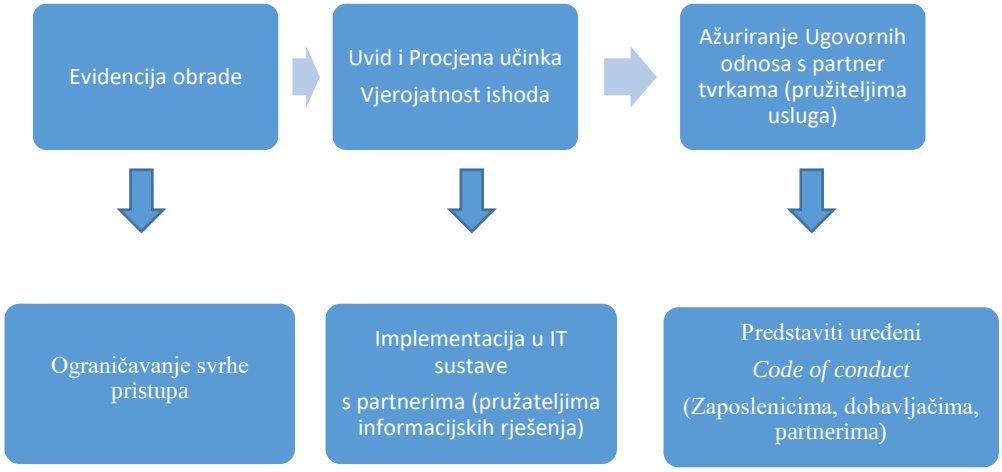
Najviše me zanimaju sljedeće teme:

- Pripreme za državnu maturu
- Visoko učilište Algebra
- Digitalna akademija
- Executive MBA - e-Leadership
- Osnove informatike
- Razvoj aplikacija
- Dizajn
- Informacijske tehnologije
- Marketing
- EU fondovi
- Knjigovodstvo
- Razvoj sadržaja
- Zelena zanimanja
- Ostala edukacija
- Specijalističke akademije
- Industrijska certifikacija
- Certifikacijski seminari

- DAJEM PRIVOLU
- NE ŽELIM DA ME KONTAKTIRATE

5.6 Praćenje usklađenosti sa regulativom u području zaštite osobnih podataka i privatnosti

Upravo iz činjenice da se svaki zaposlenik Algebra grupe susreo s prikupljanjem i/ili obradom osobnih podataka fizičke osobe važno je podići svjesnost gdje spremaju podatke osobnog identiteta. Prema navedenom, potrebno je provesti edukaciju osoblja o implementaciji GDPR-a u procese Algebra grupe sukladno predstavljenom procesu:



Slika 4. Praćenje usklađenosti Algebra grupe sukladno predstavljenom procesu

Izvor: Autorov rad

Slika 5. Identificiranje procesa usklađivanja s Uredbom

Izvor: Autorov rad

Praćenje usklađenosti sa regulativom započinje u trenutku kada implementacijski tim procjeni potrebe i razmjernosti koje mora prenijeti prvo interno te predložiti mjere za ublažavanje rizika koje su definirane nakon utvrđivanja i procjena rizika. Usklađenost Algebra grupe pratit će Službenik za zaštitu osobnih podataka usko surađujući sa voditeljima obrade, voditeljima odjela

sukladno svrsi obrade podataka, tehničkim i sigurnosnim mjerama i evidencijama o kontrolama nad tehničkim i organizacijskim mjerama. Neophodno je provoditi interni audit u definiram roku i osigurati dokumentaciju izvješće audita.

5.7 Povreda osobnih podataka

Agencija za zaštitu osobnih podataka Republike Hrvatske donosi rješenje prilikom utvrđivanja povrede Zakona o zaštiti osobnih podataka prema kojima se zabranjuje daljnja obrada, prikupljanje i brisanje osobnih podataka te zabrana iznošenja osobnih podataka iz Republike Hrvatske. U slučajevima nepostupanja u skladu s Uredbom, Agencija može pokrenuti postupak pred nadležnim prekršajnim sudom. Novčane kazne za nepoštivanje Uredbe kreću se od 20.000 do 40.000 za pravnu osobu te od 5.000 do 10.000 kuna za odgovornu osobu u toj pravnoj osobi.

Najčešći slučajevi povrede ove vrste u obradi osobnih podataka su u svrhe marketinga, zlouporaba osobnih podataka na internetu i društvenim mrežama, obrada osobnih podataka od strane financijskih institucija, nedozvoljena objava osobnih podataka, zlouporaba osobnih podataka prilikom sklapanja ugovora s teleoperaterima, zamjena identiteta (npr. krivo uparivanje OIB-a), te propusti kod obrade posebnih kategorija osobnih podataka odnosno „osjetljivih“ osobnih podataka [24]. Također, prisutna je i mogućnost zlouporabe suvremenih tehnologija kao što su prikupljanje i obrada osobnih podataka video nadzorom i biometrijom prsta.

6.Zaključak

Tehnološki napretkom i razvojem novih tehnologija postalo je nužno donošenje novog instrumenta koji će osigurati prava i temeljnu slobodu pojedinaca u vezi s obradom njihovih osobnih podataka. Nova pravila o zaštiti osobnih podataka, Opće uredba o zaštiti osobnih podataka – GDPR izravno se počinje primjenjivati u Republici Hrvatskoj od 25.svibnja 2018. godine te donosi velike promjene u društvu kao i napredak u području zaštite osobnih podataka. Temeljno pitanje koje se postavlja jest tko podliježe pravilima Uredbe, na koji način te kako se pravovaljano zaštiti od visokih kazni zbog neusklađenosti. GDPR isključivo stavlja naglasak na zaštitu osobnih podataka fizičkih osoba, stoga njezine odredbe moraju poštivati svi subjekti koji u sklopu svog poslovanja obrađuju osobne podatke fizičkih osoba u Europskoj uniji te u određenim slučajevima prema zemljama koje je Europska komisija utvrdila da su osigurale odgovarajuću razinu zaštite pojedinaca. Osobni podatak prema uredbi su: *„svi podaci koji se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi („ispitanik"); pojedinac čiji se identitet može utvrditi jest osoba koja se može identificirati izravno ili neizravno, osobito uz pomoć identifikatora kao što su ime, identifikacijski broj, podaci o lokaciji, mrežni identifikator ili uz pomoć jednog ili više čimbenika svojstvenih za fizički, fiziološki, genetski, mentalni, ekonomski, kulturni ili socijalni identitet tog pojedinca."* [25]. Nadalje, obrada navedenih osobnih podataka podrazumijeva radnje poput prikupljanja, bilježenja, čuvanja, uvida, otkrivanja, prenošenja ili uništavanja. Obrada osobnih podataka nalaže zakonitu, poštenu i transparentnu obradu s obzirom na ispitanika, a odnosi se na sve pravne subjekte, bez obzira na poslovnu djelatnost i veličinu koji u bilo kojem obliku prikupljaju, obrađuju i upravljaju osobnim podacima. Prilagodba Uredbi za organizacije predstavlja veliki izazov u implementaciji tehničkih ali i organizacijskih mjera. Cilj ovog rada bilo je predstaviti Uredbu, opisati zakonitosti kojima se vodi, pozicionirati GDPR u poslovne procese na primjeru Algebra grupe, predstaviti implementacijski plan kroz DPIA i Gap analizu te provesti program usklađenosti poslovnih procesa u organizacijsku strukturu Algebra grupe s naglaskom na odjel marketinga. Sukladno navedenom, Algebra grupa, točnije Algebra Pučko otvoreno učilište, Visoko učilište Algebra i Algebra d.o.o. subjekti su nad kojima je proveden implementacijski plan. Algebra grupa u svom poslovanju obrađuje osobne podatke s obzirom na poslovnu svrhu, ukoliko postoji jasno određena i dokumentirana zakonska osnova ili osnova temeljena na ugovornom odnosu, dok su ostale obrade dozvoljene jedino uz jasnu dokumentiranu privolu vlasnika ili njegovog opunomoćenika.

Algebra grupa prikuplja osobne podatke putem komunikacijskih kanala: telefonski, izravni kontakt, e-mailom te prijavnicom putem web obrasca te prema Uredbi, mora provesti tehničke i organizacijske mjere zaštite nad njima te osigurati da je ispitanik upoznat sa svim pravima koje ostvaruje, poput prava na: pristup, ispravak, brisanje, ograničavanje obrade, prijenos podataka i pravo na prigovor. Sukladno navedenom, prema pravnoj podlozi za provođenje obrada prikazana je evidencija obrade osobnih podataka koja predstavlja početak mjere usklađenosti za organizaciju s obzirom da se definiraju svi poslovni procesi u kojima se koriste osobni podaci. Nakon kreiranja evidencije aktivnosti obrade ili zbirke osobnih podataka potrebno je, sukladno njima definirati i poduzeti određene radnje tehničke i organizacijske naravi. Organizacijske i tehničke mjere koje Algebra grupa započela s ciljem usklađivanja uključivale su revidiranje politike zaštite osobnih podataka, predstavljeni su voditelji i izvršitelji obrade koji određuju svrhu, uvjete i način obrade osobnih podataka, provedena informacijska revizija, revidiranje ugovorne klauzule s tvrtkama partnerima, te definiranje privola s obzirom da se osobni podaci prikupljaju u marketinške, prodajne i svrhe profiliranja korisnika. Tehničke mjere uključivale su definiranje i ograničavanje pristupa podacima prema ulogama (rolama) zaposlenika u poslovnoj aktivnosti koju obavljaju. Nadalje, sinkronizirani su sustavi nad koje Algebra grupa provodi obradu osobnih podataka, uključujući sustave ALPS, Infoeduku, MyQtest i Wordpress web sajtove koji su predstavljali točke prikupljanja osobnih podataka.

Preporuke za unaprjeđenje zaštite u prikupljanju i daljnjoj obradi osobnih podataka podrazumijevaju organizacijske i tehničke mjere koje je potrebno implementirati u Algebra grupi. Organizacijske mjere sukladno zahtjevima uključuju redizajn Pravilnika o radu, Internu Politiku zaštite osobnih podataka te nove klauzule o zaštiti osobnih podataka sa partnerima i dobavljačima Algebra grupe, imenovanje DPO-a, uska suradnja DPO-a s voditeljima odjela, definiranje uloga zaposlenika koji ostvaruju pristup osobnim podacima u IT sustavima (ograničenje pristupa) sukladno poslovnoj aktivnosti, osigurati kvalitetu pristanka ispitanika kroz privolu s predstavljenom jasnom zakonitom svrhom prikupljanja osobnih podataka kao i jasnim predstavljanjem prikupljanja osobnih podataka Algebra grupe u marketinške, prodajne i svrhe profiliranja kroz sve komunikacijske kanale. Algebra grupa u skladu sa zakonskim aktima nadležnog tijela u obrazovnom sustavu (AZVO, MZO-a) podrazumijeva provedbu tehničkim mjera u vidu zaštite osobnih podataka nad IT sustavima koji provode obradu uključuju: aktiviranje forme za upit o osobnim podacima integrirati u CRM sustav, kriptiranje svih lozinku unutar sustava (ALPS, Infoeduka, MyQtest), provođenje tehničkim mjera u vidu

ograničavanja uvida u osobne podatke sukladno poslovnoj aktivnosti zaposlenika, vršenje kontrole i evidencije o fizičkom pristupu nad IT sustavima (sustav za otkrivanje neovlaštenog ulaska, sustav zaključavanja), otkrivanju podataka (zaštita prijenosa protokolima SSL/TLS za mrežnu sigurnost), sigurne pohrane podataka, održavanje, razvoj i testiranje sustava (tehnike de-identifikacije) te sigurnosno okruženje (čuvanje enkripcijskih ključeva).

Algebra grupa svoje je poslovanje započela usklađivati prema odredbama i smjernicama Uredbe imajući u vidu povrede i propuste koji su predstavljale rizik za daljnje poslovanje. U slučajevima nepostupanja u skladu s Uredbom, nadležno tijelo Republike Hrvatske, Agencija za zaštitu osobnih podataka može pokrenuti postupak pred nadležnim prekršajnim sudom, prema kojem novčane kazne za nepoštivanje Uredbe je od 20.000 kn do 40.000 kn za pravnu osobu te od 5.000 do 10.000 kuna za odgovornu osobu u toj pravnoj osobi. S obzirom na visoke novčane kazne koje Uredba propisuje, Algebra grupa svoje je poslovne modele uskladila i time potvrdila i opravdala svoju kvalitetu poslovnog modela i kvalitetu obrazovanja.

Popis slika:

Popis tablica:

Literatura

K. Plazonić, N. Šoić; Zaštita osobnih podataka, Priručnik o zakonitoj uporabi tehnologije u svrhu obrade osobnih podataka tijekom radnog odnosa, Forum Poslovni Mediji d.o.o., (2018.) ISSN: 1849-8701

Darren Wray; The Little Book of GDPR: Getting on the Path to Compliance; (2017); ISBN: 1522021140

Uredba (EU) 2016/679 Europskog parlamenta i vijeća o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju

https://ico.org.uk/ (30.05.2018)

https://edps.europa.eu/ (30.05.2018)

[1] http://www.businessinsider.com/how-to-see-where-google-knows-ive-been-2015-2 (30.05.2018)

[2] https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/ (30.05.2018)

[3,4,5,6,7,8,9,10,14,19,20,21,22,23] Uredba (EU) 2016/679 Europskog Parlamenta i vijeća

[11] https://sudreg.pravosudje.hr/registar/f?p=150:28:0::NO:28:P28_SBT_MBS:80417267 (30.05.2018)

[12] https://www.nvao.net/ (30.05.2018)

[13] https://www.algebra.hr/visoko-uciliste/o-nama/akreditacije-i-certifikati/ (30.05.2018)

[15] https://www.algebra.hr/certifikacijski-seminari/elearning/myqtest/ (30.05.2018)

[16] http://novemogucnosti.com/(30.05.2018)

[17] http://gdprandyou.ie/data-protection-impact-assessments-dpia/#what-is-a-data-protection-impact-assessment (30.05.2018)

[18] https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/

[24] http://azop.hr/info-servis/detaljnije/koji-su-najcesci-slucajevi-povrede-zakona-i-kakve-su-kazne-zbog-povrede-zak (30.05.2018)

„Pod punom odgovornošću pismeno potvrđujem da je ovo moj autorski rad čiji niti jedan dio nije nastao kopiranjem ili plagiranjem tuđeg sadržaja. Prilikom izrade rada koristio sam tuđe materijale navedene u popisu literature ali nisam kopirao niti jedan njihov dio, osim citata za koje sam naveo autora i izvor te ih jasno označio znakovima navodnika. U slučaju da se u bilo kojem trenutku dokaže suprotno, spreman sam snositi sve posljedice uključivo i poništenje javne isprave stečene dijelom i na temelju ovoga rada".

U Zagrebu, 30.05.2018.

_____