Sveučilište u Rijeci, Tehnički fakultet

AKCIJSKI PLAN
ZA IMPLEMENTACIJU GDPR UREDBE

Sveučilište u Rijeci
Tehnički fakultet

AKCIJSKI PLAN
ZA IMPLEMENTACIJU GDPR UREDBE

SADRŽAJ:

AKCIJSKI PLAN
ZA IMPLEMENTACIJU GDPR UREDBE

1. *IZVORI KORIŠTENI U IZRADI AKCIJSKOG PLANA*

- UREDBA (EU) 2016/679 EUROPSKOG PARLAMENTA I VIJEĆA od 27. travnja 2016. 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) (u daljnjem tekstu: „GDPR Uredba“);
- Uputa Sveučilišta u Rijeci sastavnicama, KLASA: 080-02/18-01/24, URBROJ: 2170-57-01-18-2 od 28. ožujka 2018. godine;
- Zakon o zaštiti osobnih podataka (NN 103/03, 118/06, 41/08, 130/11, 106/12);
- web stranica Agencije za zaštitu osobnih podataka, na linku: http://azop.hr/info-servis/detaljnije/opca-uredba-o-zastiti-podataka-gdpr;
- portal Knjižnica za zaštitu osobnih podataka www.gdpr-2018.hr

2. *NAJVAŽNIJE NOVOSTI SUKLADNO GDPR UREDBI*

Najvažnije novosti koje donosi GDPR Uredba su:

I. **Nepoštivanje odredbi znači novčanu sankciju.**

II. **Za nadzor primjene zadužena je Agencija za zaštitu osobnih podataka (AZOP).**

III. **Imenovanje službenika zaduženog za zaštitu osobnih podataka.**

IV. **Jasan pristanak osobe na korištenje njenih osobnih podataka.**

V. **Obveza promptne obavijesti prema nadležnoj službi i ispitaniku za slučaj proboja osobnih podataka.**

VI. **Dokumentiranje operativnih procedura.**

VII. **Uvođenje novih tehničkih i informatičkih rješenja u svrhu zaštite osobnih podataka.**

VIII. **Multidisciplinarni pristup problematici zaštite osobnih podataka.**

3. NAJVAŽNIJE DEFINICIJE

OSOBNI PODACI

Osobni podaci 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.

U osobne podatke potpadaju:
Ime, adresa, e-mail adresa, IP i MAC adresa, GPS lokacija, RFID tagova i kolačića na web stranicama, telefonski broj, fotografija, video snimke pojedinaca, OIB, biometrijski podaci (otisak prsta, snimka šarenice oka), genetski podaci, podaci o obrazovanju i stručnoj spremi, podaci o plaći, podaci o kreditnom zaduženju, podaci o računima u banci, podaci o zdravlju, seksualnoj orijentaciji, glas i mnogi drugi podaci koji se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi.

OBRADA OSOBNIH PODATAKA

Obrada osobnih podataka je 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.

SUSTAV POHRANE

Sustav pohrane je svaki strukturirani skup osobnih podataka dostupnih prema posebnim kriterijima, bilo da su centralizirani, decentralizirani ili raspršeni na funkcionalnoj ili zemljopisnoj osnovi.

VODITELJ OBRADE

Voditelj obrade 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. Sveučilište u Rijeci, Tehnički fakultet je voditelj obrade (u daljnjem tekstu: „Fakultet“).

PRIVOLA ISPITANIKA

Privola ispitanika znači svako 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.

POVREDA OSOBNIH PODATAKA

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.

PSEUDONIMIZACIJA

Pseudonimizacija je obrada osobnih podataka na način da se osobni podaci više ne mogu pripisati određenom ispitaniku bez uporabe dodatnih informacija, pod uvjetom da se takve dodatne informacije drže odvojeno te da podliježu tehničkim i organizacijskim mjerama kako bi se osiguralo da se osobni podaci ne mogu pripisati pojedincu čiji je identitet utvrđen ili se može utvrditi.

4. NAČELA OBRADE OSOBNIH PODATAKA

- **zakonitost, poštenost i transparentnost obrade:** to znači da obrada treba biti u skladu s određenim pravnim temeljem, a načelima poštene i transparentne obrade zahtijeva se da je pojedinac informiran o postupku obrade i njegovim svrhama, te voditelj obrade je obvezan ispitaniku pružiti sve dodatne informacije neophodne za osiguravanje poštene i transparentne obrade uzimajući u obzir posebne okolnosti i kontekst obrade osobnih podataka, a osim toga ispitanik bi trebao biti informiran o postupku izrade profila i posljedicama takve izrade profila;

- **ograničavanje svrhe:** to znači da podaci trebaju biti prikupljeni u posebne, izričite i zakonite svrhe te se dalje ne smiju obrađivati na način koji nije u skladu s tim svrhama; ali je moguća daljnja obrada u svrhe arhiviranja u javnom interesu, u svrhe znanstvenog ili povijesnog istraživanja ili u statističke svrhe;

- **smanjenje količine podataka:** to znači da podaci moraju biti primjereni, relevantni i ograničeni na ono što je nužno u odnosu na svrhe u koje se obrađuju;

- **točnost:** to znači da podaci moraju biti točni i prema potrebi ažurni; mora se poduzeti svaka razumna mjera radi osiguravanja da se osobni podaci koji nisu točni, uzimajući u obzir svrhe u koje se obrađuju, bez odlaganja izbrišu ili isprave;

- **ograničenje pohrane:** to znači da podaci moraju biti čuvani u obliku koji omogućuje identifikaciju ispitanika samo onoliko dugo koliko je potrebno u svrhe radi kojih se osobni podaci obrađuju; na dulja razdoblja čuvanja su moguća samo ako će se osobni podaci obrađivati isključivo u svrhe arhiviranja u javnom interesu, u svrhe znanstvenog ili povijesnog istraživanja ili u statističke svrhe uz provedbu primjerenih mjera zaštite propisanih Uredbom;

- **cjelovitost i povjerljivost:** to znači da podaci moraju biti obrađivani na način kojim se osigurava odgovarajuća razina sigurnosti, uključujući zaštitu od neovlaštene ili nezakonite obrade te od slučajnog gubitka, uništenja ili oštećenja;

- **pouzdanost:** to znači da je voditelj obrade odgovoran za poštivanje načela i da je teret dokaza na njemu.

5. PRAVNI TEMELJ OBRADE OSOBNIH PODATAKA

Za zakonitu obradu osobnih podataka potrebno je ispuniti barem jedno od narednih pravnih temelja:

- ispitanik je dao privolu za obradu svojih osobnih podataka u jednu ili više posebnih svrha - privola je 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, Uredbom se među ostalim utvrđuje da uvjet dobrovoljnosti nije ispunjen ako ispitanik nema istinski ili slobodan izbor ili ako nije u mogućnosti odbiti ili povući privolu bez posljedica (npr. privola se daje radi uvrštenja potrošača u neki program vjernosti, dok je u velikoj većini radnopravnih odnosa nemoguće koristiti privolu kao pravnih temelj za obradu podataka radnika);

- obrada je nužna za izvršavanje ugovora u kojem je ispitanik stranka ili kako bi se poduzele radnje na zahtjev ispitanika prije sklapanja ugovora (npr. obrada podataka tražitelja posla radi pozivanja na testiranje, obrada podataka osiguranika radi izvršenja ugovora o osiguranju ili obrada podataka radnika na poslovima održavanja instalacija radi slanja na teren);

- obrada je nužna radi poštovanja pravnih obveza voditelja obrade (npr. slanje podataka o radnicima HZZO-u ili HZMO-u ili slanje podataka stranaka od strane javnog bilježnika Poreznoj upravi sukladno posebnim propisima);

- obrada je nužna kako bi se zaštitili ključni interesi ispitanika ili druge fizičke osobe (npr. otkrivanje od strane nadležnih tijela podataka jednog roditelja drugomu radi uzdržavanja djeteta);

- obrada je nužna za izvršavanje zadaće od javnog interesa ili pri izvršavanju službene ovlasti voditelja obrade (npr. zbog službene ovlasti Državnog zavoda za statistiku pojedini voditelji obrade su dužni tom zavodu dostavljati određene osobne podatke);

- obrada je nužna za potrebe legitimnih interesa voditelja obrade ili treće strane, osim kada su od tih interesa jači interesi ili temeljna prava i slobode ispitanika koji zahtijevaju zaštitu osobnih podataka, osobito ako je ispitanik dijete, s time da se ova točka ne odnosi na obradu koju provode tijela javne vlasti pri izvršavanju svojih zadaća (npr. legitimni interes vlasnika nekretnine da postavi sustav video nazora da bi spriječio realan rizik po njegovoj imovini).

6. PROCJENA PRIPREMLJENOSTI

Prije uvođenja odredbi GDPR Uredbe u radne procese Fakulteta potrebno je utvrditi u kojoj mjeri su procesi/poslovanje unutar Fakulteta usklađeni s odredbama GDPR Uredbe.
Kako bi predmetno bilo moguće ostvariti potrebna je podrška i sudjelovanje:

- upravljačkog tijela,
- pravnika,
- službenika za zaštitu osobnih podataka,
- voditelja poslovnih procesa,
- ICT stručnjaka.

CILJEVI:

- precizno definirati zahtjeve koje GDPR Uredba i odgovarajuća nacionalna regulativa nakon 25.05.2018. godine postavlja pred Fakultet,
- utvrditi u kojoj su mjeri ti zahtjevi već zadovoljeni postojećim stanjem,

- procijeniti resurse potrebne za ostvarenje potpune sukladnosti sa zahtjevima Uredbe.

Naročito je potrebno voditi računa da su zahtjevi GDPR Uredbe multidisciplinarni, te je implementaciji iste potrebno pristupiti s aspekata pravnih zahtjeva, usklađenosti poslovnih procesa s Uredbom te podrške u vidu odgovarajućih tehničkih rješenja.

7. PRILAGODBA PROCEDURE PRIKUPLJANJA I OBRADE OSOBNIH PODATAKA

U svrhu implementacije GDPR Uredbe u procese Fakulteta, potrebno je pristupiti reviziji svih poslovnih procesa koji na bilo koji način uključuju osobne podatke obuhvaćene Uredbom GDPR.

7.1. Preduvjeti implementacije GDPR Uredbe

- Procjena rizika,
- Dokumentiranje operativnih procedura.

Nakon odrađenog prvog koraka implementacije, odnosno usporedbe postojećeg stanja zaštite osobnih podataka sa zahtjevima Uredbe potrebno je pristupiti procjeni rizika. Procjenom rizika po osobne podatke koje Fakultet prikuplja i obrađuje utvrdit će se daljnje potrebne analize utjecaja na zaštitu privatnosti, te detektirati scenariji visokog rizika.
Procese kod kojih postoji potencijalni rizik ili visoki rizik potrebno je dokumentirati, a što je preduvjet sukladnosti u slučaju revizije nadzornih tijela.

7.2. Uvođenje novih procesa

Ukoliko je za potrebu usklađenja načina prikupljanja i obrade osobnih podataka s zahtjevima GDPR Uredbe isto nužno, potrebno je uvesti i nove procese baratanja osobnim podacima.

7.3. Povrede osobnih podataka

Kako bi se potencijalne povrede osobnih podataka čim prije detektirale i otklonile, potrebno je sljedeće:

- čim ranije otkrivanje povreda osobnih podataka,
- utvrđeni načini postupanja za slučaj povreda osobnih podataka.

Komunikacijski procesi prema AZOP-u i zahvaćenim stranama kritični su za kontrolu štete i izbjegavanje sankcija prema Fakultetu.

Mehanizmi otklanjanja rizika obuhvaćaju:

- dokumentiranje procesa zaštite osobnih podataka,
- implementaciju tehničkih rješenja čuvanja podataka,
- osmišljavanje konkretnih rješenja otklanjanja potencijalnih povreda,
- osiguranje preventivnih, zaštitnih mjera za osiguranje tajnosti osobnih podataka,
- osiguranje adekvatnih informatičkih rješenja kod pokušaja kompromitiranja osobnih podataka.

7.4. Prava ispitanika (vlasnika osobnih podataka)

Prava ispitanik (vlasnika osobnih podataka) odnose se na zaposlenike i studente odnosno, vlasnike unutar Fakulteta i sve vanjske partnere, odnosno, suradnike, klijente (sve osobe čije osobne podatke Fakultet prikuplja i obrađuje).

Prava ispitanika, a o čemu će više riječi biti u daljnjem tekstu, se temelje se na čl.12. do čl.22. GDPR Uredbe. Predmetna prava obuhvaćaju pravo na informiranje ispitanika (podaci o voditelju obrade, službeniku za zaštitu osobnih podataka, svrsi obrade....), pravo na pristup (potvrda o obradi osobnih podataka ispitanika ukoliko ih voditelj obrade obrađuje....), pravo na ispravak i brisanje („pravo na zaborav“), pravo na ograničenje obrade pod točno propisanim uvjetima, pravo na prenosivost podataka (na zahtjev ispitanika voditelj obrade izdaje ispitaniku njegove osobne podatke koji ih tada ima pravo prenijeti drugom voditelju), pravo na prigovor na obradu osobnih podataka i pravo na automatizirano pojedinačno donošenje odluka (ispitanik ima pravo da se na njega ne odnosi odluka koja se temelji isključivo na automatiziranoj obradi).

7.5. Imenovanje službenika za zaštitu osobnih podataka

Prema odredbama GDPR-a, ali i trenutno važećeg Zakona o zaštiti osobnih podataka (NN 103/03, 118/06, 41/08, 130/11, 106/12), Fakultet je voditelj zbirke osobnih podataka koji zapošljava više od 20 radnika. S te osnove je Fakultet dužan imenovati službenika za zaštitu osobnih podataka.

Raspon djelovanja službenika za zaštitu osobnih podataka (zadaće sukladno čl. 39. Uredbe):

- informiranje i savjetovanje voditelja obrade ili izvršitelja obrade te zaposlenika koji obavljaju obradu o njihovim obvezama iz Uredbe te drugim odredbama Unije ili države članice o zaštiti podataka (Zakon o zaštiti osobnih podataka NN 103/03, 118/06, 41/08, 130/11, 106/12);

- praćenje poštovanja Uredbe te drugih odredaba Unije ili države članice o zaštiti podataka i politika voditelja obrade ili izvršitelja obrade u odnosu na zaštitu osobnih podataka, uključujući raspodjelu odgovornosti, podizanje svijesti i osposobljavanje osoblja koje sudjeluje u postupcima obrade te povezane revizije;

- pružanje savjeta, kada je to zatraženo, u pogledu procjene učinka na zaštitu podataka i praćenje njezina izvršavanja u skladu s člankom 35. Uredbe;

- suradnja s nadzornim tijelom (Agencija za zaštitu osobnih podataka);

- djelovanje kao kontaktna osoba za nadzorno tijelo o pitanjima u pogledu obrade, što uključuje i prethodno savjetovanje iz članka 36. Uredbe (slučajevi kada bi obrada osobnih podataka dovela do visokog rizika ukoliko se ne primjene mjere za ublažavanje rizika) te savjetovanje, prema potrebi, o svim drugim pitanjima.

8. PRAVNE PRILAGODBE

Uredba GDPR pred Fakultet postavlja pravne zahtjeve koji se mogu razmatrati kroz odnose u četiri smjera prema trećim stranama:

- Agencija za zaštitu osobnih podataka (regulatorno tijelo),

- zaposlenici,

- studenti,

- poslovni partneri i klijenti.

Regulatorno tijelo

GDPR uvodi promjene u djelokrugu rada nacionalnih regulatornih tijela u smislu preimenovanja u tzv. *Supervisory Authority* (SA) institucije na razini svake države EU. U našem slučaju to će vjerojatno ostati Agencija za zaštitu osobnih podataka – AZOP.

AKCIJSKI PLAN
ZA IMPLEMENTACIJU GDPR UREDBE

Zaposlenici

Uredba GDPR se odnosi i na osobne podatke zaposlenika.
Fakultet mora sustavno voditi evidencije prikupljenih suglasnosti zaposlenika za obradu njihovih osobnih podataka u točno određene poslovne svrhe kada to nalaže kriterij zakonitosti prikupljanja i obrade te vrste podataka.

Studenti

Uredba GDPR se odnosi i na osobne podatke studenata.
Fakultet mora sustavno voditi evidencije prikupljenih suglasnosti svojih studenata za obradu njihovih osobnih podataka u točno određene svrhe kada to nalaže kriterij zakonitosti prikupljanja i obrade te vrste podataka..

Poslovni odnosi

Fakultet mora voditi računa o svim poslovnim odnosima u kojima koristi usluge pohrane, obrade, prijenosa ili bilo kakvog drugog oblika korištenja osobnih podataka pod svojom odgovornošću.
Također je potrebno voditi računa o eventualnom prijenosu podataka: unutar i izvan Fakulteta, te naročito izvan granica EU/EEA (European Economic Area); s nizom predviđenih pravnih mehanizama i tehničkih zahtjeva.
Obaveze spram klijenata (fizičkih osoba) obuhvaćat će svih šest prava vlasnika osobnih podataka, pri čemu će njihova provedba zahtijevati znatne procesne/tehnološke izmjene.

Na ovom mjestu važno je istaknuti i najvažnija prava ispitanika (vlasnika osobnih podataka), te odredbe GDPR Uredbe iz kojih navedena prava proizlaze:

- **transparentnost (čl.12.-14.)**: pružanje informacija prilikom prikupljanja osobnih podatak kada voditelj obrade mora među ostalim informacijama obavijestiti ispitanika i o svojem identitetu i kontakt podacima, svrhama obrade i pravnoj osnovi za obradu podataka, primateljima, iznošenju u treće zemlje, razdoblju pohrane, mogućnosti povlačenja privole, itd.;
- **pristup podacima (čl.15.)**: dobiti od voditelja obrade potvrdu obrađuju li se osobni podaci koji se odnose na njega te ako se takvi osobni podaci obrađuju, pristup osobnim podacima i informacije, među ostalim, o obrađenim osobnim podacima, o svrsi obrade, roku pohrane, iznošenju u treće zemlje itd.;

- **pravo na ispravak (čl.16.)**: ispitanik ima pravo zahtijevati ispravak netočnih osobnih podataka koji se na njega odnose, a uzimajući u obzir svrhe obrade, ispitanik ima pravo dopuniti nepotpune osobne podatke, među ostalim i davanjem dodatne izjave;

- **brisanje („pravo na zaborav“) (čl.17.)**: ispitanik ima pravo od voditelja obrade ishoditi brisanje osobnih podataka koji se na njega odnose bez nepotrebnog odgađanja te voditelj obrade ima obvezu obrisati osobne podatke bez nepotrebnog odgađanja ako, među ostalim, osobni podaci više nisu nužni u odnosu na svrhu obrade, ispitanik je povukao privolu za obradu, osobni podaci su nezakonito obrađeni itd., ovo pravo ima ograničenja pa tako na primjer političar ne može zatražiti brisanje informacija o sebi koje su dane u okviru svojega političkog djelovanja;

- **pravo na ograničenje obrade (čl.18.)**: u pojedinim situacijama (na primjer kada je točnost podataka osporavana ili kada pravo na brisanju ispitanik želi da voditelj obrade zadrži njegove podatke) ispitanik ima pravo zahtijevati da se obrada ograniči uz iznimku pohrane i nekih drugih vrsta obrade;

- **pravo na prenosivost (čl.20.)**: ispitanik ima pravo zaprimiti svoje osobne podatke, a koje je prethodno pružio voditelju obrade, u strukturiranom obliku te u uobičajeno upotrebljavanom i strojno čitljivom formatu te ima pravo prenijeti te podatke drugom voditelju obrade bez ometanja od strane voditelja obrade kojem su osobni podaci pruženi, ako se obrada provodi automatiziranim putem i temelji na privoli ili ugovoru;

- **pravo na prigovor (čl.21.)**: ispitanik ima pravo uložiti prigovor na obradu osobnih podataka ako se ista temelji na zadaće od javnog interesa, na izvršavanje službenih ovlasti voditelja obrade ili na legitimne interesa voditelja obrade (uključujući i profiliranje), tada voditelj obrade ne smije više obrađivati osobne podatke ispitanika osim ako dokaže da njegovi legitimni razlozi za obradu nadilaze interese ispitanika te radi zaštite pravnih zahtjeva, također ako se ispitanik protivi obradi za potrebe izravnog marketinga, osobni podaci više se ne smiju obrađivati;

- **pravo usprotiviti se donošenju automatiziranih pojedinačnih odluka (profiliranje) (čl.22.)**: ispitanik ima pravo da se na njega ne odnosi odluka koja se temelji isključivo na automatiziranoj obradi, uključujući izradu profila, koja proizvodi pravne učinke koji se na njega odnose ili na sličan način značajno na njega utječu, osim ako je takva odluka potrebna za sklapanje ili izvršenje ugovora između ispitanika i voditelja obrade podataka, ako je dopuštena pravom EU-a ili nacionalnim pravom koji se propisuju odgovarajuće mjere zaštite prava i sloboda te legitimnih interesa ispitanika ili temeljena na izričitoj privoli ispitanika.

9.TEHNIČKE PRILAGODBE

9.1.Područja tehničke prilagodbe

Tehnička rješenja prikupljanja, čuvanja i obrade osobnih podataka moraju biti usklađena s odredbama GDPR na sljedećim područjima:

- pravovremena (unutar 72 h) prijava potencijalne ili stvarne povrede osobnih podataka prema AZOP-u (sukladno čl. 33.) i obavijest prema ispitaniku u skladu i po uvjetima iz čl.34. GDPR Uredbe,
- čuvanje podataka isključivo unutar određenog perioda (ovisno o propisanoj svrsi njihovog prikupljanja),
- transparentno i lako dostupno obavještavanje vlasnika osobnih podataka o svrsi prikupljanja, načinu obrade, roku čuvanja, njihovim pravima itd.,
- ostvarenje prava vlasnika osobnih podataka na uvid, izmjenu i brisanje podataka (ukoliko je isto moguće sukladno zakonskim propisima),
- mogućnost prenosivosti osobnih podataka (data portability),
- upravljanje privolama vlasnika osobnih podataka, uz posebne odredbe vezane uz osobne podatke djece i maloljetnika,
- implementacija „Privacy by design“ principa, odnosno, čuvanje podataka utemeljeno na zakonskom okviru, kroz zakonom utvrđeno vrijeme uz smanjenje količine podataka adekvatnim zbrinjavanjem po isteku roka čuvanja ili je gašenjem svrhe čuvanja.

9.2.Procjena postojećih ulaganja u tehnologiju

Potrebno je izvršiti procjenu postojećih tehnoloških ulaganja i njegovu usklađenost s GDPR uredbom.

Po mogućnosti se već implementirana rješenja na drugim razinama zaštite osjetljivih ili tajnih podataka mogu proširiti i na područje osobnih podataka.

Tu se prvenstveno radi o domenama automatske pretrage podataka (*e-discovery*), klasifikacije, sigurne identifikacije i autentikacije (*Identity & Access Management*, IAM), enkripcije/maskiranja podataka (anonimizacija, pseudonimizacija), nadzora aktivnosti/pristupa/ponašanja korisnika (SIEM, UBA, DLP…), upravljanja

sadržajem/dokumentima/zapisima (*Content/Document/Records Management Systems*), *Enterprise* komunikacijskim rješenjima i dr.

Kao pravni tekst, GDPR ne propisuje precizne tehničke zahtjeve (iako se mogu naknadno pojaviti u pratećim Pravilnicima), što ostavlja relativnu slobodu u odabiru i implementaciji rješenja.

Područja koja tradicionalno nisu zahtijevala tehničku podršku, a što se može uvelike promijeniti su: automatizacija izvođenja analiza utjecaja na privatnost, „mapiranje" tokova osobnih podataka (ručnim unosom ili automatiziranim praćenjem), rješenja za upravljanje privatnošću (tzv. Privacy management frameworks), website scanning alati (uključujući provjeru parametara privatnosti), upravljanje privolama, upravljanje sigurnosnim rizicima trećih strana, upravljanje incidentima (evidencija), rješenja za online privatnost (obavijesti, tracking tehnologije) itd.

10.SAMOPROCJENA USKLAĐENOSTI S GDPR UREDBOM

U svrhu utvrđenja usklađenosti trenutnog stanja zaštite osobnih podataka na Fakultetu sa zahtjevima, te planiranja daljnjih koraka prema ostvarenju potpune implementacije GDPR Uredbe potrebno je ispitati sljedeće:

1. **Temeljem Akcijskog plana izraditi tablicu procjene i realizacije zahtjeva koje pred Fakultet postavlja GDPR Uredba.**

-Predmetna tablica će pokazati koji zahtjevi po pitanju nove regulative zaštite osobnih podataka su već realizirani, a koje treba odraditi u zakonskom roku (do 25.5.2018. godine).

2. **Imenovati službenika za zaštitu osobnih podataka.**

3. **Imenovati i educirati Projektni tim za usuglašavanje mjera i procedura iz područja zaštite osobnih podataka na Fakultetu s odredbama GDPR Uredbe.**

-Projektni tim se sastoji od pravnika, službenika za zaštitu osobnih podataka, informatičkog stučnjaka, rukovoditelja odjela u čijim radnim procesima se obrađuje najveća količina osobnih podataka, a djeluje u suradnji i pod vodstvom Uprave.

4. **Jasno definirati što su osobni podaci u smislu GDPR Uredbe, te utvrditi slučajeve u kojima IP adresa, lokacijska koordinata (GPS) ili IMEI broj mogu predstavljati osobne podatke.**

-Predmetno je moguće putem kodeksa kojeg je moguće donijetu u svrhu preciziranja primjene GDPR Uredbe ili nekog drugog internog općeg akta, odnosno pravilnika (npr. Pravilnik o radu).

AKCIJSKI PLAN
ZA IMPLEMENTACIJU GDPR UREDBE

5. **Ispitati na kojim mjestima se unutar organizacijske strukture obrađuju osobni podaci, te po potrebi, dopuniti sistematizaciju radnih mjesta na način da se utvrdi koje osobne podatke, u koju svrhu i na kojem temelju može obrađivati pojedini zaposlenik te njegova odgovornost.**

-Npr. zaposlenici Službe općih i kadrovskih poslova obrađuju osobne podatke zbog prijave/odjave zaposlenika na HZZO, HZMO, tajnice zavoda obrađuju osobne podatke studenata zbog upisa ocjena na pojedinom ispitnom roku i sl.

6. **Popisati (katalogizirati) sve osobne podatke unutar Fakulteta koji se čuvaju u papirnatoj i digitalnoj formi.**

- Minimalni elementi inventure sadrže: vrsta osobnog podatka, kategorija osobnog podatka, pravna osnova, svrha i trajanje obrade, odgovorna osoba i osobe koje imaju pravo pristupa podatku, eventualni prijenos podataka ili povjeravanje obrade podataka trećim pravnim ili fizičkim osobama.

7. **Uspostaviti nove i/ili revidirati postojeće zbirke osobnih podataka i o tome obavijestiti Agenciju za zaštitu osobnih podataka.**

-Temelj za kompletiranje zbirki su podaci iz popisa osobnih podataka, a kako je to određeno u popisu (katalogu) osobnih podataka iz prethodnog zahtjeva.
Prema trenutno važećem hrvatskom zakonodavstvu, osim u iznimnim slučajevima, voditelj obrade je dužan Agenciji za zaštitu osobnih podataka dostaviti evidenciju o zbirkama osobnih podataka. Navedena obveza nestaje stupanjem na snagu Opće uredbe o zaštiti podataka, te su voditelji obrade dužni nadzornom tijelu omogućiti uvid u zbirke koje vode, na zahtjev nadzornog tijela (čl.30. GDPR Uredbe).

8. **Utvrditi da li postojeći interni akti sadrže odredbe o zaštiti osobnih podataka, te ih po potrebi nadopuniti sukladno GDPR Uredbi.**

-Osim internih akata kao što su Pravilnik o radu ili sl. način postupanja s osobnim podacima može biti razrađen i kroz procedure Sustava upravljanja kvalitetom.

9. **Izraditi kodeks ponašanja ili proširenje postojećeg kodeksa u svrhu preciziranja primjene Uredbe na način kako to propisuje čl. 40. GDPR Uredbe.**

-Izrada kodeksa je mogućnost, a ne obveza.

10. **Unijeti odgovarajuće odredbe u ugovore o radu i studiranju, te izraditi posebne obrasce privole za posebne situacije.**

11. **Prilagoditi postojeće ili uspostaviti nove procedure prema korisnicima i interne procedure koje će u okviru obavljanja radnih zadataka spriječiti uvid u osobni podatak obrada kojeg je u nadležnosti jednog radnog mjesta radnom mjestu koje nema takvih ovlaštenja.**

-Utvrditi da li je isto već uređeno procedurama Sustava upravljanja kvalitetom.

12. **Utvrditi da li Fakultet posjeduje centralni repozitorij dijela ili svih obrada osobnih podataka.**

13. **Ispitati tehničke mogućnosti za provedbu tzv. vanity search-a u kontekstu ostvarivanja prava ispitanika na transparentnost, promjenu i brisanje podataka, te povlačenje prethodno dane privole.**

-Predmetno se odnosi na mogućnost pojedinca da od Fakulteta zatraži informaciju o obradi vlastitih podataka, da zatraži brisanje vlastitih osobnih podataka iz evidencije Fakulteta ili povuče privolu za obradu istih.

14. **Ukoliko se prikupljaju osobni podaci o djeci i maloljetnicima, osigurati privolu za obradu od strane roditelja/skrbnika.**

15. **Ukoliko se osobni podaci dijele s trećim stranama na temelju ugovornog odnosa (izuzev zakonske obaveze), takvi ugovori moraju sadržavati odredbe o zaštiti osobnih podataka.**

16. **Provjeriti da li Ustanova koristi usluge u oblaku (cloud) od proizvođača sa sjedištem izvan EU/EEA (Europski ekonomski prostor).**

17. **Utvrditi/kreirati način prikupljanja privola za obradu osobnih podataka u slučajevima kada se obrada osobnih podataka temelji na privoli.**

-Privole se prikupljaju u slučajevima i kako je to propisano čl. 7. GDPR Uredbe.
Prema mišljenju AZOP-a nije potrebno prikupiti nove privole za osobne podatke koji su već u obradi ukoliko se obrada temelji na privoli na temelju Direktive 95/46/EZ te ako je način na koji je ta privola dana u skladu s uvjetima iz Opće Uredbe.

18. **Uspostaviti proces upravljanja potencijalnim povredama osobnih podataka, te iste poduprijeti tehničkim rješenjima za detekciju i odgovor na eventualne incidente.**

-Predmetno se primjerice može odnositi na uvođenje radne obveze izvan radnog vremena radi uklanjanja tehničkog rizika od proboja sustava u kojem se čuvaju osobni podaci ili pravovremenim ulaganjem u potrebna tehnička i informatička rješenja. O povredama osobnih podataka voditelj zbirke je dužan izvijestiti nadzorno tijelo i ispitanika čiji su osobni podaci povrijeđeni (čl.33. i čl. 34. GDPR Uredbe).

19. **Izvršiti procjenu postojećih mjera zaštite osobnih podataka, isto ponoviti jednom u svakih 12 mjeseci i po potrebi kreirati i uvesti nove (tehničke i informatičke mjere zaštite).**

-Na ovaj način osigurava se sigurnost i otklanja rizik od povrede osobnih podataka. Osobni podaci se trebaju zaštititi osobnim lozinkama za pristup računalima zaposlenika, aplikacijama za obradu osobnih podataka (MOZVAG, ISVU radnici, ISVU studenti, Share point i sl.). Po potrebi se može koristiti i pseudonimizacija, enkripcija osobnih podataka, a povjerljivost podataka treba biti redovno testirana. Važan moment je i ukidanje/izmjena prava pristupa

pojedinim aplikacijama ili dijelovima Share pointa nakon prestanka radnog odnosa na Fakultetu ili promjene radnog mjesta unutar organizacijske strukture. (čl.32. GDPR Uredbe).

20. Ukloniti iz papirnatih i elektroničkih evidencija sve osobne podatke za koje ne postoji osnova za obradu ili je prestala.

-Fakultet je svrstan u I. kategoriju stvaratelja arhivske građe, te se registraturna građa po isteku rokova čuvanja mora izlučiti uz suradnju s Državnim arhivom u Rijeci, a sukladno zakonskim propisima i internim aktima. Predmetno se odnosi i na dokumente koji sadrže osobne podatke, a nisu arhivska građa (ne čuvaju se trajno), npr. kolokviji, ispiti.
Materijali koji ne predstavljaju registraturnu građu, već su samo pomoćni ili radni materijali (npr. popis nastavnog ili administrativnog osoblja koji služi upisu u bazu MOZVAG, ISVU, popis studenata koji služi skidanju zabrana za pojedini ispitni rok i sl.) mogu se uništiti ili izbrisati na način da se takvi podaci ne mogu ponovno upotrijebiti. U tu svrhu je potrebna procjena tehničkih mogućnosti za tu vrstu uklanjanja takvih materijala, posebno za materijale u elektroničkom obliku (npr. brisanje, brisanje iz Recycle Bin-a), a posebno za materijale u papirnatom obliku koji se adekvatno mogu uništiti putem aparata za uništavanje papira.

21. Provesti edukaciju ili na drugi adekvatni način upoznati nastavno i administrativno osoblje, ali i studente s načinom obrade njihovih osobnih podataka i njihovim pravima i obvezama.

22. Na web-stranicama Fakulteta pod "Opći akti i dokumenti" urediti i mjesto za dokumente iz područja zaštite osobnih podataka.

-U svrhu poštivanja načela transparentnosti i lakšeg i bržeg ostvarivanja prava iz područja zaštite osobnih podataka za ispitanike, ali i za upoznavanje zaposlenika Fakulteta s područjem zaštite osobnih podataka.