

**PRAVILNIK O TEHNIČKIM I ORGANIZACIJSKIM MJERAMA ZA
OSIGURAVANJE TAJNOSTI I ZAŠTITE OBRADU OSOBNIH PODATAKA
SVEUČILIŠTA U ZAGREBU ŠUMARSKOG FAKULTETA**

SADRŽAJ:

- I. Opće odredbe
- II. Tehničke i organizacijske mjere
- III. Završne odredbe

Zagreb, 25. svibnja 2018. godine

Sukladno članku 1. stavku 1. Zakona o provedbi Uredbe o zaštiti podataka kojim se osigurava provedba Uredbe (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) (Tekst značajan za EGP) (SL L 119, 4.5.2016.) (dalje u tekstu: Opća uredba o zaštiti podataka), SVEUČILIŠTE U ZAGREBU ŠUMARSKI FAKULTET, sa sjedištem u Zagrebu, Svetošimunska cesta 25, OIB: 07699719217 ovime donosi sljedeći:

PRAVILNIK O TEHNIČKIM I ORGANIZACIJSKIM MJERAMA ZA OSIGURAVANJE TAJNOSTI I ZAŠTITE OBRADJE OSOBNIH PODATAKA

I. OPĆE ODREDBE

Predmet

Članak 1.

Ovim pravilnikom SVEUČILIŠTE U ZAGREBU ŠUMARSKI FAKULTET, sa sjedištem u Zagrebu, Svetošimunska cesta 25, OIB: 07699719217 (dalje u tekstu: FAKULTET) u svojstvu **voditelja obrade osobnih podataka** utvrđuje tehničke i organizacijske mjere za osiguravanje tajnosti i zaštite obrade osobnih podataka ispitanika.

Definicije

Članak 2.

Određeni termini korišteni u ovom pravilniku imaju sljedeće značenje:

1. **„Osobni podaci“** znači 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;

2. **„Obrada“** znači 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;
3. **„Voditelj obrade“** znači fizička ili pravna osoba, koje obrađuje osobne podatke ispitanika;
4. **„Izvršitelj obrade“** znači fizička ili pravna osoba, koje obrađuje osobne podatke u ime voditelja obrade;
5. **„Sustav pohrane“** znači svaki strukturirani skup osobnih podataka dostupnih prema posebnim kriterijima, bilo da su centralizirani, decentralizirani ili raspršeni na funkcionalnoj ili zemljopisnoj osnovi;
6. **„IT-sjecište“** je jedinstvena kontaktna točka za sve IT potrebe uključujući traženje rješenja za IT problem, podnošenje ili prosljeđivanje na višu razinu zahtjeva za podršku, kontaktiranje IT podrške;
7. **„Dokument“** je bilo koja isprava koja sadrži osobne podatke koji mogu biti u elektroničnom i materijalnom obliku, čuvani na mediju ili na informacijsko-komunikacijskoj opremi te korišteni u obradi podataka, dostavljeni putem e-maila i/ili preneseni putem elektroničke komunikacijske mreže;
8. **„Identifikacija“** je bilo koja radnja informacijskog sustava vezana uz identifikaciju ovlaštenih osoba;
9. **„Informacijska infrastruktura“** je cjelokupna informacijsko-komunikacijska mreža Fakulteta, u okviru koje se informacije prikupljaju, obrađuju i pohranjuju;
10. **„Informacijski sustav“** je svaki sustav koji se koristi u obradi osobnih podataka kako bi podaci bili lakše dostupni i primjenjivi za svakoga tko ima pravo i potrebu da ih kao takve koristi;
11. **„Incident“** je svaka nepravilnost koja utječe ili bi potencijalno mogla utjecati na tajnost i zaštitu osobnih podataka;
12. **„Kontrola pristupa“** je svaka radnja za dodjeljivanje pristupa osobnim podacima ili informacijsko-komunikacijskoj opremi ovlaštenoj osobi u svrhu kontrole;
13. **„Ispitanik“** je svaka fizička osoba na koju se obrađeni podaci odnose;

14. **„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;
15. **„Službenik za zaštitu osobnih podataka“** je osoba koja je zaposlena ili angažirana u Fakultetu, te imenovana od strane Fakulteta u smislu članka 37. Uredbe o zaštiti osobnih podataka, a koja jedina ima ovlaštenu pristup dokumentima i informacijsko - komunikacijskom sustavu Fakulteta.
16. **„Treća strana“** znači fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo koje nije ispitanik, voditelj obrade, izvršitelj obrade ni osobe koje su ovlaštene za obradu osobnih podataka pod izravnom nadležnošću voditelja obrade ili izvršitelja obrade;
17. **„Treća zemlja“** je svaka zemlja koja nije članica Europske unije ili članica Europskog gospodarskog prostora;
18. **„Lozinka“** je povjerljiva informacija koja se sastoji od broja znakova koji se koriste za provjeru ovlaštenih osoba;
19. **„Medij“** je svaki materijalni uređaj u informacijskom sustavu koji se koristi u obradi osobnih podataka i na koji se podaci mogu pohraniti ili s kojeg se podaci mogu preuzeti;
20. **„Kontrola“** je svaka radnja vezana uz provjeru ovlaštene osobe informacijskog sustava;
21. **„Sigurnosna kopija“** je svaka kopija osobnih podataka koja se nalazi u elektroničkom dokumentu koji je pohranjen na mediju u svrhu njegova preuzimanja;
22. **„Korisnik“** je svaka osoba koja ima pristup obradi osobnih podataka unutar Fakulteta.

Obrada osobnih podataka

Članak 3.

(1) Odredbe ovog pravilnika su primjenjive na:

- djelomično ili u potpunosti automatiziranu obradu osobnih podataka i
- ostalu ručnu obradu osobnih podataka kao dio stalnog prikupljanja osobnih podataka ili kojoj je namjena postati dio takvog prikupljanja osobnih podataka.

(2) Obrada, pohrana i prijenos podataka između organizacijskih jedinica Fakulteta u Republici Hrvatskoj i u inozemstvu Europskog gospodarskog prostora, kao i prijenos istih trećim osobama regulirani su politikom privatnosti Fakulteta, koja je u skladu sa zakonom Republike Hrvatske, a prema tome i s pravilima Europske unije.

II. TEHNIČKE I ORGANIZACIJSKE MJERE

Članak 4.

(1) Fakultet primjenjuje tehničke i organizacijske mjere koje pružaju sigurnost i zaštitu obrade osobnih podataka u skladu s prirodom obrađenih podataka i potencijalnim rizicima za vrijeme obrade.

Tehničke mjere

Članak 5.

(1) Prilikom automatske obrade podataka poduzimaju se sljedeće tehničke mjere za zaštitu obrade osobnih podataka:

Svaka osoba zaposlena/angažirana od strane Fakulteta ima na raspolaganju odvojeno osobno (prijenosno) računalo za izvršavanja radnih zadataka i pristup odvojenoj radnoj stanici. Radna stanica je radni prostor namijenjen za dugotrajni uredski posao koji izvršava jedna osoba, s vodoravnom radnom površinom, podesivom radnom stolicom te pristupom električnoj energiji, podacima i telefonu, a nalazi se u prostorima općih uredskih radnih jedinica.

(2) Jedinствено korisničko ime i lozinka zahtijevaju pristupnu lozinku od 12 (dvanaest) znakova za prijavu u operacijski sustav Windows te e-mail račun. Prijenosna računala imaju isto korisničko ime i lozinku za Windows i za e-mail. Osim zadane duljine pristupna lozinka mora sadržavati 3 od 5 vrsta znakova: velika slova, mala slova, simbole, brojeve i unicode znakove (općenite međunarodne znakove). Jedinствена lozinka stvorena od strane svake zasebne ovlaštene osobe na računalu, koje se koristi za radne zadatke, a koje računalo je u vlasništvu Fakulteta, pod pretpostavkom da svaka osoba zaposlena/angažirana od strane Fakulteta ima različitu lozinku za računalo koje je u vlasništvu Fakulteta, samo za računalo dano na raspolaganje od strane Fakulteta za izvršavanje radnih zadataka, pod pretpostavkom da:

- lozinka dozvoljava pristup osobi zaposlenoj od strane Fakulteta samo dijelovima sustava koji su joj potrebni za izvršavanje radnih zadataka;

- lozinka je tajna te se ne smije davati trećim osobama izvan Fakulteta ni pod kojim uvjetima, niti se smije davati međusobno između osoba zaposlenih/ angažiranih od strane Fakulteta;
- nijedna osoba zaposlena/angažirana od strane Fakulteta ne smije koristiti računalo druge osobe zaposlene/angažirane od strane Fakulteta i koje je dano na raspolaganje od strane Fakulteta za izvršavanje radnih zadataka; i
- Fakultet periodično mijenja pristupne lozinke. Svi računi za interakciju s korisnicima imaju postavljen rok trajanja od najviše 3 (tri) mjeseca;
- u slučaju sumnje da su osobni podaci ugroženi, lozinke računa za usluge će se smjesta promijeniti.

(3) Automatska odjava iz sustava na svakom zasebnom osobnom računalu nakon isteka određenog perioda neaktivnosti od 15 (petnaest) minuta te je za ponovnu aktivaciju sustava na osobnom računalu potrebno ponovno unijeti lozinku.

(4) Ako se korisnik ne uspije prijaviti (unosom nevažećeg korisničkog imena ili lozinke) u sustav nakon 3 (tri) pokušaja, isti će kontaktirati Službenika za zaštitu osobnih podataka koja će zatražiti podršku za izmjenu lozinke od „IT-sjecišta“.

(5) Učinkovit i siguran antivirusni i protušpijanski program instaliran na svakom prijenosnom računalu na Fakultetu, redovito ažuriran putem internetske veze s najnovijim zaštitnim definicijama u svrhu zaštite od nepoznatih i nepredvidivih prijetnji od novih virusa i sl. IT sjedište zahtijeva da svi sustavi imaju instaliran odobreni antivirusni softverski paket s najnovijom ažuriranom verzijom. Fakultet koristi antivirusni softver po operativnom sustavu. Radne stanice, osobna računala i prijenosna računala s Windowsom (32 i 64 bitna verzija) koriste AVG Antivirus FREE. Na ulazu u fakultetsku mrežnu infrastrukturu postavljen je firewall FORTIGATE 300D sa pokrenutim antivirusom.

(6) Bilježenje i čuvanje odgovarajuće dokumentacije za softver za obradu osobnih podataka i svih promjena;

(7) Instalacija usmjerivača između informacijskog sustava i interneta kao zaštitna mjera protiv neovlaštenog i/ili zlonamjernog pokušaja ulaska i/ili proboja u sustav;

(8) Ako postoji potreba za korištenjem računala izvan prostorija društva Fakulteta (rad od kuće, sastanak, itd.), tada se primjenjuju prikladne sigurnosne mjere za danu situaciju (VPN i enkripcija);

(9) Spajanje opreme u sobi za informatičku tehnologiju (IT) na energetska mrežu putem uređaja za neprekidno napajanje (UPS).

(10) Sustav kontrole temperature u IT sobi, u kojoj se nalazi oprema;

(11) Protupožarni sustav u prostorima Fakulteta, fizička zaštita i pristup opremi uređeni su detaljno u skladu sa standardima računalne sigurnosti Fakulteta;

(12) Licencirani programi – Microsoft (uključujući sve programe potrebne za rad na računalu za izvršavanje zadataka) za sva računala koja se koriste za potrebe Fakulteta i koja su u vlasništvu istog, uključujući antivirusne i protušpijunske sustave. Svi programi potrebni za rad su instalirane osobe koje su zaposlene/angažirane od strane Fakulteta uz mogućnost pomoći od strane „IT-sjedišta“. Samovoljna instalacija programa, aplikacija i slično od strane osoba koje je zaposlio/angažirao Fakultet, a da instalaciju istih nije odobrila uprava Fakulteta, je zabranjena;

(13) Osobe zaposlene/angažirane od strane Fakulteta imaju pravo osigurati dnevno održavanje (ažuriranje softvera, 1 razina provjere) njihovih osobnih računala s mogućnošću pristupa od strane „IT-sjedišta“ za održavanje i popravke velikih problema, ali cijeli sustav računala je vlasništvo Fakulteta. Svaki popravak odnosno održavanje osobnih računala se bilježi te se izvješće dostavlja „Glavnom sjedištu“.

(14) Za vrijeme prikupljanja osobnih podataka putem web stranice Fakulteta, ispitaniku se pruža jednostavna, jasna i nedvosmislena obavijest da unosom podataka ona/on pristaje na politike zaštite privatnosti te zaštite i prijenosa osobnih podataka. Takvi podaci se čuvaju zasebno te se za potrebe statistike anonimiziraju u roku od 6 (šest) mjeseci od prikupljanja.

Dodatne tehničke mjere

Članak 6.

(1) Dodatne tehničke i organizacijske mjere za vrijeme obrade osobnih podataka omogućuju:

1. Klasifikaciju osobnih podataka na osnovnu, srednju i visoku razinu tajnosti, kao i određivanje pristupa grupi podataka i načina ophođenja istom;
2. Prepoznavanje svakog zasebnog pristupa informacijskom sustavu putem verifikacije i autorizacije svake ovlaštene osobe;
3. Ograničen pristup za sve ovlaštene osobe samo onim bazama podataka ili osobnim podacima koji su potrebni za izvršavanje poslovnih zadataka;

4. Enkripciju podataka koji se mogu prenijeti putem telekomunikacijske mreže (internetska mreža, bežične mreže) ili bilo koja druga vrsta veze s odgovarajućim softverom i tehničkim mjerama.

Sigurnosne kopije

Članak 7.

(1) Sigurnosne su kopije obvezne na kraju svakog radnog dana i radnog tjedna te se kreiraju putem automatiziranog sustava sigurnosnih kopija osobnih računala.

(2) Dohvat podataka sa sigurnosnih kopija vrši se u skladu s politikom IT kontinuiteta i politikom upravljanja IT rizikom te posebice od strane ovlaštene osobe u „IT-Sjecištu“.

(3) Sigurnosne se kopije čuvaju na sigurnim, neobjavljenim lokacijama unutar sjedišta Fakulteta. Točne lokacije se ne objavljuju i poznate su samo imenovanoj odgovornoj osobi za GDPR u društvu.

Prijenos podataka

Članak 8.

(1) Prijenos osobnih podataka vrši se na sljedeći način:

1. Kod materijalnog oblika (tiskana kopija – papir) uvijek pazi da dokumenti koji sadrže osobne podatke nisu vidljivi trećim osobama te ih se dostavlja samo ovlaštenim osobama, posebice kada se isti nose izvan prostorija Fakulteta te se na taj način osigurava da se takvi podaci ne otkrivaju neovlaštenim osobama;

2. Kod prijena osobnih podataka u elektroničkom obliku putem medija za prijenos podataka, podaci se štite, ovisno o obliku podataka, lozinkom i enkripcijom;

Članak 9.

(1) U slučaju da se prikupljanje osobnih podataka provodi putem web stranice Fakulteta, ispitanik je putem objavljenih pravila obaviješten o pravilima zaštite osobnih podataka i privatnosti te mu se moraju pružiti sve ostale potrebne informacije, kao što je određeno Uredbom, otvaranjem zasebnog prozora ili zasebne, lako dostupne poveznice na istoj stranici na kojoj je potreban unos podataka.

(2) Jezik i način obavještavanja prilagođeni su široj publici, a da pritom nije potrebno koristiti nepotrebne tehničke ili stručne termine.

Organizacijske mjere

Članak 10.

(1) Odgovorne osobe društva Fakulteta poduzimaju organizacijske mjere za zaštitu automatske obrade osobnih podataka na način da obavještavaju upravu društva i ovlaštene osobe, osiguravaju fizičku zaštitu radnih prostora i opreme te zaštitu informacijskog sustava u cijelosti, uključujući i prijenos podataka.

(2) Osoba odgovorna za praćenje regulacija koje se odnose na zaštitu osobnih podataka i obavještavanje uprave društva i/ili zaposlenika u pogledu provedbe zaštite osobnih podataka, odgovorna za koordinaciju i kontrolu postupaka i vođenje predviđena u dokumentaciji tehničkih i organizacijskih mjera je Službenik za zaštitu osobnih podataka. Njemu/njoj će pomoći osoba odgovorna za IT sjecište.

Sigurnosni video nadzor

Članak 11.

(1) Sustav video nadzora koristi se zbog zaštite zaposlenika i svih drugih osoba koje se nađu u prostorima sjedišta Fakulteta. Sustav se nadalje koristi i za sprječavanje protupravnih radnji usmjerenih prema imovini Fakulteta (krađe, oštećenja, uništenja i sl). Pri tome Fakultet može koristiti usluge stručnih podizvođača (zaštitarskih službi) koji također imaju svojstvo izvršitelja obrade.

(2) Sustav sigurnosnog video nadzora uspostavlja se i obavlja u skladu sa Zakonom o privatnoj zaštiti (NN 68/03, 31/10, 139/10), Pravilnika o uvjetima i načinu provedbe tehničke zaštite u odgovarajućoj aktualnoj verziji te u člankom 25.-32. Zakona o provedbi Opće uredbe o zaštiti podataka (NN42/18).

(3) Fakultet označava da je objekt odnosno pojedina prostorija u njemu te vanjska površina objekta pod video nadzorom, a oznaka je vidljiva najkasnije prilikom ulaska u perimetar snimanja. Fakultet ne obavlja djelatnost praćenja i snimanja javnih površina.

(4) Oznaka o video nadzoru koja se izrađuje u obliku naljepnice ili pločice sadrži sljedeće podatke:

1. lako razumljivu sliku uz tekst kojim se ispitanicima pružaju sljedeće informacije:

- da je prostor pod video nadzorom
- podatke o voditelju obrade
- podatke za kontakt putem kojih ispitanik može ostvariti svoja prava.

(5) Pravo pristupa osobnim podacima prikupljenim putem video nadzora ima:

- odgovorna osoba u sjecištu video nadzora;
- službenik za zaštitu osobnih podataka; te

- uprava društva.

(6) Fakultet posjeduje automatizirani sustav zapisa za evidentiranje pristupa snimkama video nadzora koji će sadržavati vrijeme i mjesto pristupa, kao i oznaku osoba koje su izvršile pristup podacima prikupljenim putem video nadzora. Snimke iz sustava video nadzora se ne smiju koristiti suprotno svrsi utvrđenoj u stavku 1. ovog članka. Sustav video nadzora zaštićen je od pristupa neovlaštenih osoba.

(7) Snimke dobivene putem video nadzora mogu se čuvati najviše 6 (šest) mjeseci, osim ako je drugim zakonom propisan duži rok čuvanja ili ako su dokaz u sudskom, upravnom, arbitražnom ili drugom istovrijednom postupku.

(8) Ukoliko je Fakultet voditelj obrade, tada društvo primjenjuje sve obveze koje iz Opće uredbe za zaštitu podataka i Zakona o provedbi Opće uredbe za zaštitu podatka koje se tiču voditelja obrade, a ukoliko Fakultet prikuplja i obrađuje osobne podatke u ime i za račun vlasnika objekta, tada se na Fakultet primjenjuju odredbe koje se tiču izvršitelja obrade podataka.

(9) Ako je vjerojatno da će obrada podataka prikupljenih videonadzorom, uzimajući u obzir prirodu, opseg, kontekst i svrhe obrade, prouzročiti visok rizik za prava i slobode pojedinaca, voditelj obrade prije obrade provodi procjenu učinka predviđenih postupaka obrade na zaštitu osobnih podataka. Pri provođenju procjene učinka na zaštitu podataka voditelj obrade traži savjet od službenika za zaštitu podataka.

(10) Ispitanici čiji osobni podaci se nalaze na videosnimkama imaju sljedeća prava:

- a) Ispitaniku se na njegov zahtjev moraju dati informacije o prikupljenim podacima, načinu čuvanja tih podataka, osobama koje imaju pristup tim podacima te trajanju čuvanja tih podataka.
- b) Ispitanik može zatražiti brisanje snimaka koje predstavljaju njegove osobne podatke te se tom traženju mora udovoljiti u najkraćem mogućem roku, a najkasnije u roku od 30 (trideset) dana od dana podnošenja zahtjeva, osim u slučajevima kada se snimka čuva radi korištenja kao dokaz u sudskom postupku.
- c) Ispitanik može zatražiti ograničenje obrade i neprenosivost njegovih snimaka koje sadrže osobne podatke, čemu će Fakultet putem Službenika za zaštitu osobnih podataka udovoljiti bez odgađanja, osim u slučajevima kada se snimka čuva radi korištenja kao dokaz u sudskom postupku.
- d) Ispitanik može uložiti prigovor na obradu njegovih osobnih podataka putem video nadzora na za to određeni kontakt.

(11) Voditelj obrade će se savjetovati s nadzornim tijelom prije obrade ako bi se procjenom učinka na zaštitu podataka iz ovog članka pokazalo da bi, u slučaju da voditelj obrade ne donese mjere za ublažavanje rizika, obrada dovela do visokog rizika.

(12) Obrada, čuvanje i prosljeđivanje snimaka koje sadrže osobne podatke dozvoljena je isključivo u svrhu očuvanja javne sigurnosti, progona radi počinjenja kaznenih djela, identifikacije štetnika radi ostvarenja prava na naknadu štete, a sve u rokovima koji su propisani odgovarajućim zakonskim propisima. Osobe koje se nalaze na snimkama koje se koriste u sudskim postupcima moraju biti obaviještene o tome da će se snimke na kojima se nalaze biti izdvojene i prosljeđene nadležnim tijelima. Zabranjeno je prosljeđivati snimke osobama koje tvrde da namjeravaju pokrenuti neki sudski postupak. Snimke se prosljeđuju isključivo po nalogu suda ili nadležnih tijela.

Video nadzor radnih prostorija

Članak 12.

(1) Sustav video nadzora koristi se zbog zaštite sigurnosti zaposlenika Fakulteta te uz izričitu privolu zaposlenika Fakulteta.

(2) Snimke koje su snimljene sustavom video nadzora mogu se isključivo koristiti za navedeno u stavku 1. ovoga članka.

(3) Video nadzorom pokriveni su prostori Fakulteta unutar zgrada na adresi Svetošimunska cesta 25 i adresi Svetošimunska cesta 23, te zgrade NPŠO-a Lipovljani i Zalesina. Pokriven je ulazni prostor i unutarnji hodnici. Video nadzorom nisu pokriveni prostori radnih mjesta, ureda sa radnim mjestima, svlačionice za zaposlenike i studente i toaletni prostori.

(4) Prilikom korištenja video nadzora poduzimaju se mjere vidljivog označavanja da je objekt odnosno pojedina prostorija u njemu pod video nadzorom, a oznaka treba biti vidljiva najkasnije prilikom ulaska u perimetar snimanja.

(5) Obavijest iz stavka 4. ovog članka sadrži posebno jednostavnu i lako razumljivu sliku uz tekst kojim se ispitanicima pružaju sljedeće informacije:

- da je prostor pod video nadzorom,
- podatke o voditelju obrade,
- kontakt podatke putem kojih ispitanik može ostvariti svoja prava.

(6) Pravo pristupa osobnim podacima prikupljenim putem video nadzora ima odgovorna osoba zaposlena kod Fakulteta, a koja je nadležna za video nadzor.

(7) Osoba iz prethodnog stavka ne smije koristiti snimke iz sustava video nadzora suprotno njihovoj utvrđenoj svrsi.

(8) Sustav video nadzora zaštićen je od pristupa neovlaštenih osoba.

(9) O snimkama video nadzora postoji sustav logova za evidentiranje pristupa snimkama video nadzora koji sadrži vrijeme i mjesto pristupa kao i oznaku osoba koje su izvršile pristup podacima prikupljenim putem video nadzora.

(10) Snimke dobivene putem video nadzora mogu se čuvati najviše 60 (šezdeset) dana osim ako je zakonom propisan duži rok čuvanja ili ako su dokaz u sudskom, upravnom, arbitražnom ili drugom istovrijednom postupku, a za što je potrebna posebna odluka odgovorne osobe društva Fakulteta za svaku pojedinu snimku, a o čemu će biti obaviještena svaka osoba koja se nalazi na predmetnoj snimci.

Fizička dokumentacija

Članak 13.

(1) Fizička dokumentacija osoba se čuva u sjedištu Fakulteta u zasebnim mapama i regulatorima zaštićenima u zasebnim ormarićima otpornima na vodu i vatru do kojih je pristup ograničen te se popis s brojevima regulatora kao i imena svake osobe, a koji podliježe zaštiti osobnih podataka, čuva u elektroničkom obliku na računalnoj mreži Fakulteta, a pristup istom je dozvoljen samo ovlaštenim osobama.

(2) Dokumenti svih osoba u fizičkom obliku se čuvaju i ne uništavaju, a elektronički oblici istih su pohranjeni na računalima. O načinu čuvanja osobnih dokumenata sastavlja se protokol te se imenuje ovlaštena osoba koja je odgovorna za njihovo čuvanje, odnosno Službenik za zaštitu osobnih podataka.

(3) Prilikom sklapanja ugovora s fizičkim osobama Fakultet će ishoditi njihovu izričitu suglasnost na prikupljanje, obradu i čuvanje osobnih podataka, pogotovo ako se navedeni ugovori prosljeđuju u svrhu obrade i čuvanja trećim osobama. Za ugovorne odnose sa fizičkim osobama, pristup osobnim podacima isključivo ima Službenik za zaštitu podataka, koji je isključivo nadležan za odgovaranje na sve upite predmetnih ispitanika. Službenik za zaštitu osobnih podataka vodi zasebnu evidenciju obrade.

(4) Sve ovlaštene osobe Fakulteta su upoznate s pravilima obrade, pohranjivanja (čuvanja) i pristupa podacima, a svaka ovlaštena osoba dužna je voditi osobnu evidenciju obrade podataka na zasebnoj datoteci na osobnom računalu.

(5) Razdoblje čuvanja dokumenata ispitanika osobnih podataka iznosi najmanje 5 (pet) godina u skladu sa odgovarajućim zakonskim propisima vezano uz bilo koji oblik osobnih podataka (od 5 godina do trajnog čuvanja).

(6) Nakon isteka roka čuvanja predmetne dokumentacije Fakultet će istu uništiti rezačima papira za uništavanje nepotrebnih papira, materijala i podataka te na taj način spriječiti bacanje dokumenata izvan prostorija.

(7) Dostava dokumenata koji su uručeni i/ili dostavljeni strankama Fakulteta ili kojim drugim ispitanicima se izvršava zatvorenom kuvertom s točno navedenim imenom i prezimenom/titulom ispitanika kojemu se dostavlja kuverta, a primitak se potvrđuje potpisom.

(8) Svi podaci navedeni u dokumentima izrađenim od strane Fakulteta, a koji se dostavljaju nadležnom sudu, upravnom tijelu, ministarstvu i drugim institucijama ili drugim korisnicima izdaju se isključivo u skladu sa zakonom ili po primitku izričite pisane privole ispitanika.

Neposredno korištenje osobnih podataka u radnim procesima

Članak 14.

(1) Fakultet posjeduje zasebnu sobu za sastanke za primanje trećih osoba izvan Fakulteta te će na taj način onemogućiti pristup radnim prostorima u Fakultetu trećim osobama koje nisu u pratnji radnika Fakulteta ili bilo koji drugi kontakt (fizički ili vizualni) takvim osobama s osobnim podacima, datotekama i drugim dokumentima.

(2) Izjava o povjerljivosti je izjava koju potpisuje radnik te se čuva u osobnom spisu radnika. Životopisi kandidata za postojeća ili buduća radna mjesta čuvaju se samo uz izričitu privolu ispitanika u zasebnoj datoteci među datotekama radnika Fakulteta.

(3) Fakultet provodi neprekidno obavještavanje ovlaštenih osoba voditelja za neposredne obveze i odgovornosti za zaštitu osobnih podataka.

Školovanje radnika

Članak 15.

(1) Prije početka rada radnici/osobe angažirane od strane Fakulteta upoznati će se sa obvezama čuvanja osobnih podataka prilikom obrade te s cjelokupnom dokumentacijom tehničkih i organizacijskih mjera te potpisuju izjavu kojom potvrđuju da prihvaćaju obveze i odgovornost vezane uz zaštitu osobnih podataka, a naznačena izjava je sastavni dio Ugovora o radu.

(2) U ugovore o radu / ugovore o angažmanu za provođenje radova u Fakultetu uključene su obveze i odgovornosti za zaštitu osobnih podataka te svaki radnik mora pristupiti odgovarajućim uvodnim treninzima uz neke dodatne treninge, ovisno o njihovom poslu, kako bi se osigurali specifični uvjeti za zaštitu osobnih podataka.

(3) Službenik za zaštitu osobnih podataka redovito (u razdobljima od tri mjeseca) se informira o novostima s područja zaštite osobnih podataka radi aktualizacije njegovih saznanja o novijoj normativnoj aktivnosti zakonodavca i upravnih tijela, a stečena znanja prenosi na ostale radnike unutar Fakulteta.

Mjere prilikom neposrednog kontakta sa ispitanicima

Članak 16.

(1) U izvršavanju ugovornih obveza Fakultet prikuplja osobne podatke putem svojih djelatnika ili podizvođača (zaštitarskih službi) u svojstvu izvršitelja obrade na način da od nasumično odabranih osoba koja pristupi u zgradu Fakulteta zatraži osobnu iskaznicu i zapiše ime i prezime te broj osobne iskaznice. Tu usluge Fakultet obavlja u svojstvu izvršitelja obrade.

(2) Fakultet će za vrijeme obrade osobnih podataka iz stavka 1. ovog članka poduzeti sljedeće dodatne tehničke i organizacijske mjere:

1. Prije prikupljanja osobnih podataka, svaka će se osoba obavijestiti o:

- cilju;
- načinu obrade osobnih podataka;
- voditelju i izvršitelju;
- pravilima privatnosti;
- načinu i razdoblju čuvanja;
- prijenosu podataka;
- pravima i obvezama voditelja, izvršitelja i ispitanika; te
- mogućnosti podnošenja pritužbe Agenciji za zaštitu osobnih podataka.

2. Svaka osoba koja neposredno prikuplja osobne podatke mora se ispitaniku predstaviti osobnim imenom i prezimenom.

3. Svaka osoba koja od ispitanika neposredno prikuplja osobne podatke mora voditi računa o opsegu osobnih podataka koje prikuplja, tj. da prikuplja samo onaj opseg osobnih podataka koji je nužan za ispunjenje svrhe u koju se osobni podaci prikupljaju (načelo razmjernosti), a sve kako se ne bi prikupljali osobni podaci u prekomjernom opsegu.

4. Na zahtjev ispitanika/građana, odnosno njihovih zakonskih zastupnika ili punomoćnika ovlaštena osoba dužna je najkasnije u roku od 30 (trideset) dana od podnošenja zahtjeva omogućiti ostvarivanje prava ispitanika/građana na uvid u njihove osobne podatke, odnosno dostaviti obavijesti, izvratke, potvrde i ispile u vezi osobnih podataka koji se obrađuju.

5. Svaki ispitanik ima pravo od voditelja obrade ishoditi brisanje osobnih podataka koji se na njega odnose bez nepotrebnog odgađanja, a o tome je Fakultet kao voditelj obrade dužan upoznati svakog ispitanika.
6. Osobni podaci iz stavka 1. ovog članka zapisuju se u bilježnicu u jednom primjerku, koja bilježnica se nakon završetka smjene čuva u zaključanoj prostoriji.
7. Nakon izvršenja naloga odnosno popunjavanja svih listova bilježnice iz prethodnog stavka, ista se dostavlja Službeniku za zaštitu osobnih podataka uz zapisnik o primopredaji. Fakulteta ili njegovi zaposlenici ne smiju koristiti niti prosljeđivati podatke iz navedene evidencije.

Povreda osobnih podataka (incident)

Članak 17.

- (1) U slučaju povrede osobnih podataka Službenik za zaštitu osobnih podataka bez nepotrebnog odgađanja i, ako je izvedivo, najkasnije 72 sata nakon saznanja o toj povredi, izvješćuje odgovornu osobu Fakulteta, dekana, te Agenciju za zaštitu osobnih podataka, i to o povredi osobnih podataka, osim ako nije vjerojatno da će povreda osobnih podataka prouzročiti rizik za prava i slobode pojedinaca.
- (2) Ako izvještaj iz prethodnog stavka nije podnesen unutar 72 sata, isti će biti popraćen obrazloženim razlozima za kašnjenje.
- (3) Voditelj „IT sjecišta“ će bez nepotrebnog odgađanja izvijestiti odgovornu osobu (dekana) Fakulteta i Službenika za zaštitu osobnih podataka nakon što sazna za povredu osobnih podataka.
- (4) U izvješćivanju iz stavka 1. će se:
 - (a) opisati priroda incidenta, uključujući, ako je moguće, kategorije i približan broj dotičnih ispitanika te kategorije i približan broj dotičnih evidencija osobnih podataka;
 - (b) navesti ime i kontaktne podatke službenika za zaštitu podataka ili druge kontaktne točke od koje se može dobiti još informacija;
 - (c) opisati vjerojatne posljedice incidenta;
 - (d) opisati mjere koje je voditelj obrade poduzeo ili predložio poduzeti za rješavanje problema povrede osobnih podataka, uključujući prema potrebi mjere umanjivanja njezinih mogućih štetnih posljedica.

(5) Službenik za zaštitu osobnih podataka dokumentira sve povrede osobnih podataka, uključujući činjenice vezane za povredu osobnih podataka, njezine posljedice i mjere poduzete za popravljjanje štete. Ta će dokumentacija nadzornom tijelu omogućiti provjeru poštivanja procedura za prijavu povrede osobnih podataka.

Obavješćivanje ispitanika o povredi osobnih podataka (incidentu)

Članak 18.

(1) U slučaju povrede osobnih podataka koje bi mogao prouzročiti visok rizik za prava i slobode pojedinaca, Službenik za zaštitu osobnih podataka bez nepotrebnog odgađanja obavješćuje ispitanika o povredi osobnih podataka.

(2) Obavješćivanjem ispitanika iz stavka 1. ovog članka opisuje se priroda povrede osobnih podataka uporabom jasnog i jednostavnog jezika te ono sadržava barem informacije i mjere iz članka 17. stavka 4. točka (b), (c) i (d).

Nadzor

Članak 19.

(1) Nadzor nad provedbom zakona sukladno Uredbi za zaštitu osobnih podataka i Zakonu o provedbi Opće uredbe o zaštiti podataka u Republici Hrvatskoj ima Agencija za zaštitu osobnih podataka.

(2) Fakultet je dužan omogućiti Agenciji za zaštitu osobnih podataka pristup spisima i drugoj dokumentaciji te sredstvima obrade osobnih podataka.

III. ZAVRŠNE ODREDBE

Stupanje na snagu

Članak 20.

Ovaj pravilnik stupa na snagu u cijelosti te proizvodi pravne učinke s danom 25. 05. 2018. godine.

Prestanak važenja

Članak 21.

(1) Ovaj pravilnik prestaje važiti donošenjem novog pravilnika za tehničke i organizacijske mjere za zaštitu tajnosti i obrade osobnih podataka.

(2) Dođe li do izmjene Zakona o zaštiti osobnih podataka kao i ostalih internih akata nakon stupanja na snagu ovog pravilnika, a iste su protivne ovom

pravilniku, poduzeti će se mjere za donošenje novog pravilnika, odnosno usklađivanje s novim odredbama.

DEKAN

prof. dr. sc. Vladimir Jambrekić, v. r.