

U skladu s Općom Uredbom EU 2016/679 i Zakonom o provedbi Opće uredbe o zaštiti podataka (NN 42/18) Predsjedništvo Akademije tehničkih znanosti Hrvatske na svojoj 7. sjednici održanoj 15. listopada 2018. donosi

PRAVILNIK O PRIKUPLJANJU, OBRADI I ZAŠTITI OSOBNIH PODATAKA

I. Opće odredbe

Članak 1.

Ovim Pravilnikom u Akademiji tehničkih znanosti Hrvatske (dalje u tekstu: HATZ) uređuju se opći postupci i mjere zaštite osobnih podataka koji se vode u zbirkama osobnih podataka kojima rukuje HATZ. Pravilnik obuhvaća opće mjere zaštite zbirke osobnih podataka tijekom njihovog prikupljanja, obrade, pohrane, prijenosa i korištenja. Svrha Pravilnika je osigurati sukladnost djelovanja Voditelja obrade s propisima na području zaštite osobnih podataka.

U postupku prikupljanja, obrade i zaštite osobnih podataka primjenjuju se odredbe Opće Uredbe EU 2016/679 (u daljnjem tekstu: Uredba) i Zakona o provedbi Opće uredbe o zaštiti podataka (NN 42/18) (u daljnjem tekstu: Zakon).

Prema odredbama Uredbe i Zakona HATZ je voditelj obrade osobnih podataka koji određuje svrhu i sredstva obrade osobnih podataka u skladu s nacionalnim zakonodavstvom i pravom Europske unije.

Podaci o voditelju obrade: **Akademija tehničkih znanosti Hrvatske**

Kačićeva 28

10 000 Zagreb

tel: 01-4922-559

fax: 01-4922-569

email: hatz@hatz.hr

Članak 2.

Pojmovi koji se koriste u Pravilniku, a imaju rodni značaj, bez obzira na to koriste li se u muškom ili ženskom rodu, obuhvaćaju na jedraki način muški i ženski rod.

U skladu s Uredbom pojedini izrazi u ovom Pravilniku imaju sljedeće značenje:

1. **Osobni podatak** je svaki podatak koji se odnosi 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 skupovima osobnih podataka, bilo automatiziranim ili 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. **Sustav pohrane** znači svaki strukturirani skup osobnih podataka dostupnih prema posebnim kriterijima, bilo da su centralizirani, decentralizirani ili raspršeni na funkcionalnoj ili zemljopisnoj osnovi.
4. **Voditelj obrade** znači 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.
5. **Izvršitelj obrade** znači fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo koje obrađuje osobne podatke u ime voditelja obrade.
6. **Primatelj** znači fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo kojemu se otkrivaju osobni podaci neovisno o tome je li on treća strana.
7. **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.
8. **Privola** ispitanika znači svako dobrovoljno, posebno, informirano i nedvosmisleno izražavanje želja ispitanika, kojim on izjavom ili jasnom potvrdnom radnjom daje pristanak na obradu osobnih podataka koji se na njega odnose.
9. **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 i na drugi način obrađivani.

II. Obrada osobnih podataka

Članak 3.

Pravilnik utvrđuje pravila povezana sa zaštitom pojedinaca u pogledu prikupljanja i obrade osobnih podataka i pravila povezana sa slobodnim kretanjem osobnih podataka.

Cilj Pravilnika je uspostaviti primjerene procese zaštite i upravljanja osobnim podacima ispitanika, odnosno članova, zaposlenika, vanjskih suradnika i drugih osoba čiji se osobni podaci obrađuju.

Pravilnik se primjenjuje na sve obrade osobnih podataka unutar HATZ-a, a temeljem pravne osnove ili privole. Pravna osnova za prikupljanje i obradu osobnih podataka su zakonski i podzakonski akti, opći akti HATZ-a i ugovori.

Privola je izražavanje želja ispitanika kojim on izjavom ili jasnom potvrdnom radnjom daje pristanak za obradu osobnih podataka koji se na njega odnose i ista se može u svakom trenutku povući. Povlačenje privole ne utječe na zakonitost obrade na temelju privole prije njezina povlačenja.

Osobne podatke fizičkih osoba HATZ obrađuje zakonito, pošteno i transparentno s obzirom na ispitanika.

Osobni podaci prikupljaju se u posebne, izričite i zakonite svrhe te se ne obrađuju na način koji nije u skladu s tako određenom svrhom.

Prikupljaju se i obrađuju samo osobni podaci koji su primjereni, relevantni i ograničeni na ono što je nužno s obzirom na svrhu za koju se obrađuju. Osobni podaci koje HATZ obrađuje su točni te se po potrebi ažuriraju. Osobni podaci koji nisu točni bez odlaganja se brišu ili ispravljaju.

HATZ osobne podatke obrađuje isključivo na način kojim se osigurava odgovarajuća sigurnost osobnih podataka, uključujući zaštitu od neovlaštene ili nezakonite obrade te od slučajnog gubitka, uništenja ili oštećenja primjenom odgovarajućih tehničkih ili organizacijskih mjera.

HATZ osobne podatke čuva samo onoliko dugo koliko je potrebno u svrhe radi kojih se osobni podaci obrađuju. Iznimno, osobni podaci mogu se pohraniti i na dulja razdoblja, ali samo ako će se isti obrađivati isključivo u svrhe arhiviranja u javnom interesu, u svrhe znanstvenog ili povijesnog istraživanja ili u statističke svrhe.

Voditelj obrade osobne podatke obrađuje u skladu sa sljedećim načelima: zakonitost, točnost, svrhovitost, trajnost, sigurnost, transparentnost.

❖ Zakonitost

Načelo zakonitosti podrazumijeva obrađivanje osobnih podataka ispitanika sukladno važećim zakonima i pokrivajući sva prava ispitanika.

❖ Točnost

Načelo točnosti podrazumijeva da osobni 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.

Voditelj obrade osigurava primjenu načela točnosti na način da ispitanik može zatražiti ispravak osobnih podataka koje je dostavio, ukoliko primijeti da neki od njegovih osobnih podataka nije ispravno naveden.

❖ Svrhovitost

Načelo svrhovitosti podrazumijeva da osobni podaci moraju biti primjereni, relevantni i ograničeni na ono što je nužno u odnosu na svrhe u koje se obrađuju.

Osobni podaci moraju biti prikupljeni u posebne izričite i zakonite svrhe te se dalje ne smiju obrađivati na način koji nije u skladu s tim svrhama.

Iznimno, daljnja obrada u svrhe arhiviranja u javnom interesu, u svrhe znanstvenog ili povijesnog istraživanja ili u statističke svrhe ne smatra se neusklađenom s prvotnim svrhama.

❖ Trajnost

Načelo trajnosti podrazumijeva da osobni podaci moraju biti čuvani u obliku koji omogućuje identifikaciju ispitanika samo onoliko dugo koliko je potrebno da se zadovolji svrha zbog koje su podaci prikupljeni.

Osobni podaci mogu se pohraniti na dulja razdoblja ukoliko je isto zakonskim aktima propisano.

❖ Sigurnost

Načelo sigurnosti podrazumijeva da osobni podaci moraju biti zaštićeni od neovlaštenog pristupa i uporabe, gubitka, uništenja ili oštećenja primjenom odgovarajućih tehničkih ili organizacijskih mjera.

❖ Transparentnost

Načelo transparentnosti podrazumijeva da će Voditelj obrade prilikom prikupljanja osobnih podataka pružiti ispitaniku sve potrebne informacije i na zahtjev osigurati ispitaniku uvid u njegove podatke, obrazloženje obrade, temelj i zakonitost obrade i slično.

Članak 4.

HATZ prikuplja i obrađuje sljedeće osobne podatke:

1. ime i prezime, adresa, osobni identifikacijski broj (OIB), datum i godina rođenja, broj telefona, e-pošta, informacije o vrsti ugovornog odnosa i sadržaju, i drugi podaci koji su posebnim propisima propisani kao nužni za (a) članstvo u HATZ-u, (b) radi zasnivanja i ostvarivanja prava iz radnog odnosa, (c) prava iz drugih ugovornih odnosa, kao i zbog (d) prijave radnika na mirovinsko i zdravstveno osiguranje.
2. Ostale osobne podatke koje ispitanik ili treća osoba stavljaju na znanje prilikom biranja u članstvo HATZ-a, zasnivanja i trajanja radnog odnosa ili drugog ugovornog odnosa, kao što su broj bankovnog računa, podaci s osobne iskaznice, stručna sprema, druga znanja i vještine.

Kategorije ispitanika i vrste podataka koji se obrađuju prikazani su u tablici 1.

Tablica 1. Kategorije ispitanika i vrste podataka

Kategorija ispitanika	Vrste podataka koji se obrađuju
I. Članovi HATZ-a	ime i prezime; dan, mjesec i godina rođenja, mjesto rođenja; OIB; znanstveni stupanj, znanstveno i znanstveno-nastavno zvanje, osobna fotografija; kućna adresa; adresa e-pošte; broj telefona; mjesto zaposlenja; naziv odjela HATZ-a kojem pripada; kategorija članstva u HATZ-u; naziv funkcije u HATZ-a; objavljeni radovi
II. Zaposlenici HATZ-a	ime i prezime; dan, mjesec i godina rođenja; mjesto rođenja; OIB; kućna adresa; adresa e-pošte; broj telefona; državljanstvo; radno iskustvo; IBAN (broj tekućeg računa); podaci s osobne iskaznice; stručna sprema; druga znanja i vještine; podaci o uzdržavanim članovima obitelji zaposlenika
III. Vanjski suradnik HATZ-a (podaci potrebni za sklapanje ugovora)	ime i prezime; OIB; kućna adresa; adresa e-pošte; broj telefona; IBAN (broj žiro računa); mjesto zaposlenja
IV. Dobitnici nagrade HATZ-a	ime i prezime; OIB; kućna adresa; adresa e-pošte; broj telefona; IBAN (broj žiro računa); mjesto zaposlenja

Voditelj obrade se u skladu s odredbama Uredbe obvezuje poštivati načela obrade osobnih podataka.

Ako se obrada osobnih podataka provodi u ime voditelja obrade, voditelj obrade koristi se jedino izvršiteljima obrade koji u dovoljnoj mjeri jamče provedbu odgovarajućih tehničkih i organizacijskih mjera na način da je obrada u skladu sa zahtjevima iz ove Uredbe i da se njome osigurava zaštita prava ispitanika.

Izvršitelj obrade ne smije angažirati drugog izvršitelja obrade bez prethodnog posebnog ili općeg pisanog odobrenja voditelja obrade.

Obrada koju provodi izvršitelj obrade uređuje se ugovorom ili drugim pravnim aktom u skladu s odredbama Uredbe.

Osobni podaci uzimaju se neposredno od ispitanika usmeno i pisanim putem ili iz drugih izvora.

Članak 5.

HATZ obrađuje osobne podatke samo ako je ispunjen jedan od sljedećih uvjeta:

1. ispitanik je dao privolu za obradu svojih osobnih podataka u jednu ili više posebnih svrha,
2. obrada je nužna za izvršavanje ugovora kojih je ispitanik stranka,
3. obrada je nužna radi poštovanja pravnih obveza voditelja obrade,
4. obrada je nužna kako bi se zaštitili ključni interesi ispitanika ili druge fizičke osobe,
5. obrada je nužna za izvršavanje zadaće od javnog interesa ili pri izvršavanju službene ovlasti voditelja obrade,
6. obrada je nužna za potrebe legitimnih interesa voditelja obrade ili treće strane, osim kad su od tih interesa jači interesi ili temeljna prava i slobode ispitanika koji zahtijevaju zaštitu osobnih podataka.

Članak 6.

Privola kojom ispitanik daje HATZ-u pristanak na obradu osobnih podataka koji se na njega odnose je dobrovoljna, u pisanom obliku, lako razumljivog, jasnog i jednostavnog jezika s jasno naznačenom svrhom.

Ispitanik ima pravo u svakom trenutku povući svoju privolu te ga se o tome prije davanja privole obavješćuje. Povlačenje privole ispitanik je ovlašten dati na jednostavan način na koji je privolu i dao.

Članak 7.

Prilikom prikupljanja osobnih podataka od ispitanika HATZ na odgovarajući način (usmeno ili pisanim putem) ispitaniku pruža informacije o svrsi obrade, pravnom temelju obrade, razdoblju u kojem će podaci biti pohranjeni, pravu ispitanika na pristup, ispravak ili brisanje osobnih podataka, pravo na ulaganje prigovora i dr.

U slučaju da se podaci ne prikupljaju izravno od ispitanika, uz navedene podatke navodi se i izvor osobnih podataka.

Pravo na ispravak

Ispitanik ima pravo bez nepotrebnog odgađanja ishoditi od HATZ-a ispravak netočnih osobnih podataka koji se na njega odnose.

Uzimajući u obzir svrhe obrade, ispitanik ima pravo dopuniti nepotpune osobne podatke, među ostalim i davanjem dodatne izjave.

Pravo na brisanje

Ispitanik ima pravo od HATZ-a ishoditi brisanje osobnih podataka koji se na njega odnose, a HATZ je obvezan obrisati osobne podatke bez nepotrebnog odgađanja ako je ispunjen jedan od sljedećih uvjeta:

1. osobni podaci više nisu nužni u odnosu na svrhe za koje su prikupljeni ili na drugi način obrađeni;
2. ispitanik povuče privolu na kojoj se obrada temelji, a ne postoji druga pravna osnova za obradu;
3. ispitanik uloži prigovor na obradu, a legitimni razlozi za realizaciju prava na brisanje imaju veću težinu od legitimnog interesa Voditelja obrade za obradu i/ili čuvanje osobnih podataka;
4. osobni podaci nezakonito su obrađeni;
5. osobni podaci moraju se brisati radi poštovanja pravne obveze.

Pravo na ograničenje obrade

Ispitanik ima pravo od HATZ-a tražiti ograničenje obrade u slučaju da (1) osporava točnost osobnih podataka, (2) kada smatra da je obrada nezakonita te se protivi brisanju osobnih podataka i umjesto toga traži ograničenje njihove upotrebe, (3) kada HATZ više ne treba osobne podatke za potrebe obrade te (4) u slučaju kada je ispitanik uložio prigovor na obradu i očekuje potvrdu nadilaze li legitimni razlozi HATZ-a razloge ispitanika.

Pravo na prenosivost podataka

Ispitanik ima pravo zaprimiti osobne podatke koji se odnose na njega, a koje je pružio HATZ-u u strukturiranom, uobičajeno upotrebljavanom i strojno čitljivom formatu te ima pravo prenijeti te podatke drugom Voditelju obrade. Potrebno je uzeti u obzir da se pravo prijenosa odnosi isključivo na osobne podatke ispitanika.

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. HATZ u takvoj situaciji više ne smije obrađivati osobne podatke osim ako dokaže da postoje uvjerljivi legitimni razlozi za obradu koji nadilaze interese, prava i slobode ispitanika ili radi postavljanja, ostvarivanja ili obrane pravnih zahtjeva.

Ukoliko se osobni podaci obrađuju za potrebe izravnog marketinga, ispitanik u svakom trenutku ima pravo uložiti prigovor na obradu osobnih podataka koji se odnose na njega za potrebe takvog marketinga, što uključuje izradu profila u mjeri koja je povezana s takvim izravnim marketingom. Ako se ispitanik protivi obradi za potrebe izravnog marketinga, osobni podaci više se ne smiju obrađivati u takve svrhe.

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 ta odluka:

1. potrebna za sklapanje ili izvršenje ugovora između ispitanika i HATZ-a,
2. dopuštena zakonom i
3. temeljena na izričitoj privoli ispitanika.

III. Druga prava ispitanika

Članak 8.

Osobni podaci ispitanika su njegovo vlasništvo i podaci koji su potrebni HATZ-u neophodni su za odvijanje osnovne djelatnosti, a ispitanici u svakom trenutku zadržavaju određena prava u odnosu na obradu njihovih podataka. HATZ prikuplja i obrađuje podatke samo uz postojanje navedenih zakonitosti obrade.

HATZ će na zahtjev ispitanika ili njegovog zakonskog zastupnika ili punomoćnika odmah, a najkasnije u roku od mjesec dana od podnošenja zahtjeva:

1. informirati o svrsi obrade njegovih osobnih podataka, kategorijama osobnih podataka koje se obrađuju, o primateljima ili kategorijama primatelja kojima su osobni podaci otkriveni ili će im biti otkriveni, predviđenom razdoblju za koje će se osobni podaci čuvati, te u slučaju kad se osobni podaci ne prikupljaju od ispitanika o njihovom izvoru,

2. dostaviti ispitaniku ispis osobnih podataka sadržanih u sustavu pohrane koji se na njega odnose,
3. ispraviti netočne podatke i/ili ih dopuniti,
4. provesti brisanje osobnih podataka koji se odnose na ispitanika pod uvjetom da osobni podaci više nisu nužni u odnosu na svrhe za koje su prikupljeni ili ako ispitanik povuče privolu na kojoj se obrada temelji.

Rok iz st. 2. ovog članka može se produljiti za dodatnih dva mjeseca, uzimajući u obzir složenost i broj zahtjeva. HATZ će obavijestiti podnositelja zahtjeva o svakom takvom produljenju u roku od mjesec dana od podnošenja zahtjeva kao i o razlozima za produljenje.

Ako zahtjev iz st. 1. ovog članka bude odbijen HATZ će najkasnije u roku od mjesec dana od podnošenja zahtjeva obavijestiti ispitanika o razlozima odbijanja zahtjeva.

Članak 9.

HATZ informacije pružene u skladu sa čl. 8. pruža bez naknade. Iznimno, ako su zahtjevi ispitanika očito neutemeljeni ili pretjerani od ispitanika će se naplatiti razumna naknada uzimajući u obzir administrativne troškove pružanja informacija ili obavijesti.

Članak 10.

Ispitanik koji smatra da su mu povrijeđena neka prava zajamčena Uredbom ima pravo podnijeti zahtjev za utvrđivanje povrede prava nadležnom tijelu.

U slučaju povrede osobnih podataka HATZ bez nepotrebnog odgađanja i, ako je izvedivo, najkasnije 72 sat nakon saznanja o toj povredi, izvješćuje nadležno nadzorno tijelo o povredi osobnih podataka, osim ako nije vjerojatno da će povreda osobnih podataka prouzročiti rizik za prava i slobode pojedinaca. Ako izvješćivanje nije učinjeno unutar 72 sata, mora biti popraćeno razlozima za kašnjenje.

Izvršitelj obrade bez nepotrebnog odgađanja izvješćuje voditelja obrade nakon što sazna za povredu osobnih podataka.

U izvješćivanju iz stavka 2. mora se barem:

1. opisati priroda povrede osobnih podataka, uključujući, ako je moguće, kategorije i približan broj dotičnih ispitanika te kategorije i približan broj dotičnih evidencija osobnih podataka,
2. navesti ime i kontaktne podatke službenika za zaštitu podataka ili druge kontaktne točke od koje se može dobiti još informacija,
3. opisati vjerojatne posljedice povrede osobnih podataka,
4. 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.

HATZ kao voditelj obrade dokumentira sve povrede osobnih podataka, uključujući činjenice vezane za povredu osobnih podataka, njezine posljedice i mjere poduzete za popravljivanje štete.

U slučaju povrede osobnih podataka koji će vjerojatno prouzročiti visok rizik za prava i slobode pojedinaca, HATZ bez nepotrebnog odgađanja obavješćuje ispitanika o povredi osobnih podataka.

Obavješćivanje ispitanika iz prethodnog stavka nije obvezno ako je ispunjen bilo koji od sljedećih uvjeta:

1. HATZ je poduzeo odgovarajuće tehničke i organizacijske mjere zaštite i te su mjere primijenjene na osobne podatke pogođene povredom osobnih podataka, posebno one koje osobne podatke čine nerazumljivima bilo kojoj osobi koja im nije ovlaštena pristupiti, kao što je enkripcija,

2. HATZ je poduzeo naknadne mjere kojima se osigurava da više nije vjerojatno da će doći do visokog rizika za prava i slobode ispitanika,
3. time bi se zahtijevao nerazmjerni napor. U takvom slučaju mora postojati javno obavješćivanje ili slična mjera kojom se ispitanici obavješćuju na jednako djelotvoran način.

IV. Službenik za zaštitu osobnih podataka

Članak 11.

Predsjednik HATZ-a imenuje službenika za zaštitu osobnih podataka zasebnom odlukom te su njegovi podaci i kontakti objavljeni na službenim web stranicama HATZ-a.

Službenik za zaštitu osobnih podataka ima odgovarajuću stručnu spremu, te su njegove zadaće sljedeće:

1. informiranje i savjetovanje voditelja obrade ili izvršitelja obrade te zaposlenika koji obavljaju obradu o njihovim obvezama iz Uredbe i Zakona, i drugih odredaba Unije i nacionalnog zakonodavstva;
2. prati poštivanje Uredbe i drugih odredaba Unije, Zakona 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 revizije;
3. pružanje savjeta, kada je to zatraženo, u pogledu procjene učinka na zaštitu podataka i praćenje njezina izvršavanja u skladu s čl. 35. Uredbe;
4. surađuje s Agencijom za zaštitu osobnih podataka;
5. djeluje kao kontaktna točka za Agenciju za zaštitu osobnih podataka o pitanjima u pogledu obrade.

Članak 12.

HATZ osigurava da je službenik za zaštitu podataka na primjeren način i pravodobno uključen u sva pitanja u pogledu zaštite osobnih podataka, te da su mu omogućena potrebna sredstva za izvršavanje njegovih zadaća.

Ispitanici mogu kontaktirati službenika za zaštitu podataka u pogledu svih pitanja povezanih s obradom svojih osobnih podataka i ostvarivanja svojih prava iz ove Uredbe.

Službenik za zaštitu podataka obavezan je čuvati povjerljivost svih podataka i informacija koje sazna u obavljanju svoje dužnosti, a ta obveza traje i nakon prestanka obavljanja dužnosti službenika za zaštitu osobnih podataka.

Službenik za zaštitu podataka može ispunjavati i druge zadaće i dužnosti. Voditelj obrade ili izvršitelj obrade osigurava da takve zadaće i dužnosti ne dovedu do sukoba interesa.

V. Mjere za zaštitu osobnih podataka

Članak 13.

HATZ provodi odgovarajuće tehničke i organizacijske mjere za omogućavanje učinkovite zaštite osobnih podataka od slučajnog gubitka, uništenja, nedopuštenog pristupa, promjene, objavljivanja ili svake druge zlouporabe.

Uzimajući u obzir najnovija dostignuća, troškove provedbe te prirodu, opseg, kontekst i svrhu obrade, kao i rizik različitih razina vjerojatnosti i ozbiljnosti za prava i slobode pojedinaca, HATZ i izvršitelj obrade provode odgovarajuće tehničke i organizacijske mjere kako bi osigurali odgovarajuću razinu sigurnosti s obzirom na rizik, uključujući prema potrebi:

1. pseudonimizaciju i enkripciju osobnih podataka,
2. sposobnost osiguravanja trajne povjerljivosti, cjelovitosti, dostupnosti i otpornosti sustava i usluga obrade
3. sposobnost pravodobne ponovne uspostave dostupnosti osobnih podataka i pristupa njima u slučaju fizičkog ili tehničkog incidenta,
4. proces za redovito testiranje, ocjenjivanje i procjenjivanje učinkovitosti tehničkih i organizacijskih mjera za osiguravanje sigurnosti obrade.

HATZ i izvršitelj obrade poduzimaju mjere kako bi osigurali da svaki pojedinac koji djeluje pod odgovornošću HATZ-a ili izvršitelja obrade, a koji ima pristup osobnim podacima, ne obrađuje te podatke ako to nije prema uputama voditelja obrade, osim ako je to obavezan učiniti prema pravu Unije ili pravu države članice.

Osobni podaci koji se pohranjuju u pisanom obliku čuvaju se u registratorima, u zaključanim ormarima. Osobni podaci koji se pohranjuju na informatičkim medijima pohranjuju se uporabom metoda i sustava zaštite koje jamče sigurnost i tajnost tako pohranjenih metoda.

Ukoliko je vjerojatno da će određena vrsta obrade, osobito putem novih tehnologija i uzimajući u obzir prirodu, opseg, kontekst i svrhe obrade, prouzročiti visok rizik za prava i slobode pojedinaca, HATZ prije obrade provodi procjenu učinka predviđenih postupaka obrade za zaštitu osobnih podataka. Jedna procjena može se odnositi na niz sličnih postupaka obrade koji predstavljaju slične visoke rizike.

Prema potrebi HATZ provodi preispitivanje kako bi procijenio je li obrada provedena u skladu s procjenom učinka na zaštitu podataka barem onda kada postoji promjena u razini rizika koji predstavljaju postupci obrade.

Voditelj obrade ima pravo zatražiti nadzor nad radnjama na podacima i nadzor nad prijenosom podataka kada smatra da je isto potrebno. Voditelj obrade dužan je provjeravati kako se prikupljaju i čuvaju privole te ima li potrebe za promjenama izjava o privatnosti (sadrži pravnu osnovu za prikupljanje, period čuvanja i pravo na prigovor nadležnom tijelu u slučaju povrede prava).

Članak 14.

Ukoliko voditelj obrade odredi izvršitelje obrade, oni su dužni:

1. obrađivati podatke samo po nalogu Voditelja obrade,
2. imati potpisane izjave o povjerljivosti,
3. čuvati zapise o obradi,

4. implementirati odgovarajuću zaštitu,
5. dobiti privolu u slučaju podugovaranja,
6. surađivati s Voditeljem obrade kod prijave povrede, zahtjeva za pristup i procjena učinka na zaštitu privatnosti,
7. imati ugrađene principe privatnosti u dizajn.

HATZ kao Voditelj obrade obavezan je s Izvršiteljima obrade imati pisani ugovor.

HATZ i izvršitelji obrade su dužni uništiti podatke nakon proteka roka predviđenog internim aktima HATZ-a, važećim prisilnim propisima ili kada prestane svrha zbog koje su osobni podaci obrađivani. HATZ vodi evidenciju aktivnosti obrade za koje je odgovoran za osobne podatke koji se stalno obrađuju odnosno za one podatke čija obrada nije povremena.

Ta evidencija sadržava sve sljedeće informacije:

1. ime i kontaktne podatke voditelja obrade i službenika za zaštitu podataka;
2. svrhu obrade;
3. opis kategorija ispitanika i kategorija osobnih podataka;
4. kategorije primatelja kojima su osobni podaci otkriveni ili će im biti otkriveni, uključujući primatelje u trećim zemljama ili međunarodne organizacije;
5. eventualne prijenose osobnih podataka u treću zemlju ili međunarodnu organizaciju, uključujući identificiranje te treće zemlje ili međunarodne organizacije te, u slučaju prijenosa iz članka 49. stavka 1. drugog podstavka Uredbe, dokumentaciju o odgovarajućim zaštitnim mjerama
6. ako je to moguće, predviđene rokove za brisanje različitih kategorija podataka;
7. ako je moguće, opći opis tehničkih i organizacijskih sigurnosnih mjera iz članka 32. stavka 1. Uredbe.

Evidencije iz prethodnog stavka moraju biti u pisanom obliku, uključujući elektronički oblik.

HATZ kao Voditelj obrade, na zahtjev daje nadzornom tijelu uvid u evidenciju.

VI. Završne odredbe

Članak 15.

Pravilnik stupa na snagu i primjenjuje se danom donošenja.

Predsjednik:

Prof. dr. sc. Vladimir Androć

