Newsletter Nacionalnog CERT-a – CERT info

Sadržaj

Tema mjeseca: Zaštita osobnih podataka

Danas, kad je gotovo svaki aspekt našeg života povezan s internetom, zaštita osobnih podataka postala je važnija nego ikad. Zaštita osobnih podataka u Hrvatskoj regulirana je Zakonom o provedbi Opće uredbe o zaštiti podataka (NN42/2018) (GDPR). Opća uredba primjenjuje se izravno u svim državama članicama Europske unije odnosno zemljama Europskog gospodarskog prostora (to su uz zemlje članice EU Norveška, Island i Lihtenštajn) od 25. svibnja 2018. godine i postavlja visoke standarde zaštite privatnosti građana.

Sukladno GDPR-u, obrada podataka mora biti zakonita i transparentna, svrha prikupljanja podataka jasno definirana, prikupljati se smiju samo oni podaci koji su zaista i potrebni za postizanje svrhe, podaci se smiju čuvati samo onoliko dugo koliko je to potrebno te moraju biti poduzete sve mjere za njihovu zaštitu.

Za nadzor provedbe GDPR-a, u Hrvatskoj, zadužena je **Agencija za zaštitu osobnih podataka (AZOP)**. AZOP pruža smjernice o pravilnoj obradi podataka, nadzire primjenu zakona i obrađuje pritužbe građana, ali ima i ovlasti izricanja kazni za nepoštivanje njezinih odredbi. Više o djelokrugu AZOP-a možete pročitati ovdje.

azop Agencija za zaštitu osobnih podataka

U ovom broju newslettera zagrepst ćemo površinu ove složene teme i istražiti kako pravilno zaštititi svoje osobne podatke, koja su vaša prava prema GDPR-u te što učiniti ako smatrate da je došlo do povrede vaše privatnosti.

O temi mjeseca razgovarali smo i s **izv.prof.dr.sc. Tihomirom Katulićem**, profesorom pravnih znanosti na Katedri za pravo informacijskih tehnologija i informatiku Pravnog fakulteta Sveučilišta u Zagrebu, čiji intervju svakako preporučujemo da pročitate.

Koja su vaša prava?

Mnogi građani nisu upoznati sa svojim pravima. Prema Općoj uredbi o zaštiti podataka (GDPR), imate pravo na:

1. **Pristup podacima**
   Imate pravo znati koje vaše osobne podatke organizacije prikupljaju, obrađuju i pohranjuju.
2. **Ispravak podataka**
   Ako su vaši podaci netočni ili nepotpuni, imate pravo zatražiti njihov ispravak.
3. **Brisanje podataka (primjer pravo na zaborav)**
   Možete tražiti brisanje vaših podataka kada oni više nisu potrebni ili ako je obrada nezakonita.
4. **Ograničenje obrade**
   Možete zatražiti privremeno ograničenje obrade podataka, primjerice dok se provjerava njihova točnost.
5. **Prigovor na obradu**
   Imate pravo prigovoriti na obradu vaših podataka, osobito kada se oni koriste za potrebe izravnog marketinga.
6. **Prijenos podataka**
   Imate pravo zatražiti da se vaši podaci prenesu drugoj organizaciji (voditelju obrade) u strukturiranom i čitljivom obliku.
7. **Povlačenje privole**
   Ako ste dali privolu za obradu podataka, imate pravo u bilo kojem trenutku povući tu privolu.
8. **Pravo u vezi automatizirano pojedinačno donošenje odluka**
   Imate pravo da se na vas ne odnosi odluka koja se temelji isključivo na automatiziranoj obradi, uključujući izradu profila, koja proizvodi pravne učinke koji se na vas odnose ili na sličan način značajno utječu na vas.

Što možemo učiniti za zaštitu svojih osobnih podataka?

Za zaštitu osobnih podataka potrebno je svakodnevno promišljanje i oprez kako bi se očuvala privatnost i spriječila njihova zloupotreba. Evo nekoliko savjeta kako pravilno zaštititi svoje osobne podatke:

1. **Čuvajte osobne dokumente** – Osobne iskaznice, putovnice i ostale dokumente držite na sigurnom mjestu i nikada ih ne dijelite s neovlaštenim osobama.
2. **Budite oprezni na internetu** – Nikada ne dijelite osobne podatke putem nepoznatih web stranica, društvenih mreža ili e-mailova sumnjivog sadržaja.

3. **Koristite snažne lozinke** – Svaki račun mora imati jedinstvenu lozinku, a kako bi ona bila dobra kombinirajte velika i mala slova, brojeve i simbole, a pobrinite se da bude i dovoljno duga.
4. **Provjerite dozvole aplikacija** – Prije instalacije aplikacija, provjerite koje dozvole traže i dijelite samo podatke koji su nužni.
5. **Aktivirajte dvofaktorsku autentifikaciju (2FA)** – Ova dodatna razina sigurnosti smanjuje rizik od neovlaštenog pristupa vašim računima.
6. **Šifrirajte osjetljive podatke** – Ako dijelite podatke putem e-maila ili drugih kanala, koristite šifriranje radi dodatne zaštite.
7. **Pažljivo čitajte pravila privatnosti** – Prije nego što date svoju privolu za obradu podataka, proučite kako će se oni koristiti.

Zaštita osobnih podataka u digitalnom okruženju

Kako bi zaštitili svoje osobne podatke u digitalnom okruženju, potrebno je voditi računa o **digitalnim tragovima** i **kibernetičkoj higijeni**.

Što su digitalni tragovi?

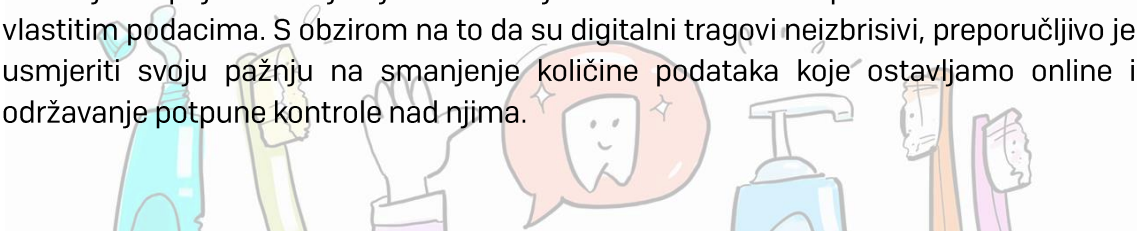
Digitalni tragovi obuhvaćaju sve informacije koje ostavljamo online – bilo da je riječ o svjesnim radnjama poput objava na društvenim mrežama ili nesvjesnim podacima koji se prikupljaju tijekom naših online aktivnosti. Svaki klik, komentar, spremljena stranica ili objavljena fotografija ostavlja otisak u digitalnom prostoru.

Zbog toga je važno pažljivo razmisliti prije nego što podijelimo osobne podatke, komentiramo ili postavljamo sadržaj. Naš digitalni trag može značajno utjecati na našu privatnost, a time i na našu sigurnost u online okruženju. Osim toga, prisutnost na internetu nije samo pitanje osobne sigurnosti, već i kontrole nad našim podacima i informacijama.

Što je kibernetička higijena?

Kako bismo sačuvali svoju privatnost i sigurnost, potrebno je usvojiti temelje kibernetičke higijene. To uključuje redovito ažuriranje softverskih sustava i uređaja, korištenje jakih lozinki, dvofaktorske autentifikacije i postavljanje sigurnosnih postavki na društvenim mrežama i aplikacijama. Obratite pažnju na to što i s kime dijelite kako bi zadržali kontrolu nad svojom privatnosti.

Zaštita privatnosti na internetu nije samo preventivna mjera protiv krađe identiteta ili financijskih prijevara. Riječ je o očuvanju osobne slobode i prava na kontrolu nad vlastitim podacima. S obzirom na to da su digitalni tragovi neizbrisivi, preporučljivo je usmjeriti svoju pažnju na smanjenje količine podataka koje ostavljamo online i održavanje potpune kontrole nad njima.



Pametno korištenje interneta, uz svijest o digitalnim tragovima, omogućuje nam da uživamo u svim prednostima digitalnog svijeta uz minimalne rizike. Pravilnim pristupom zaštiti privatnosti i sigurnosti, ne samo da štitimo sebe, već i doprinosimo sigurnijem i odgovornijem digitalnom okruženju za sve korisnike.

Što ako smatramo da je došlo do povrede naše privatnosti?

Ako sumnjate da je došlo do povrede vaših osobnih podataka, poduzmite sljedeće korake:

1. **Obratite se voditelju obrade podataka**
   Pisanim putem se obratite organizaciji koja obrađuje vaše podatke te navedite konkretan problem, zatražite njegovo uklanjanje te povratno očitovanje na navode u vašem zahtjevu.
2. **Kontaktirajte Agenciju za zaštitu osobnih podataka (AZOP)**
   Ako voditelj obrade podataka ne postupi prema vašem zahtjevu ili se na njega ne očituje, AZOP-u možete podnijeti službeni Zahtjev za utvrđivanje povrede prava.
3. **Zahtjev mora biti razumljiv i potpun**
   Proučite AZOP-ove upute kako biste podnijeli razumljiv i potpun zahtjev.

Zaštita osobnih podataka temeljno je pravo svakog građanina, a informiranost o svojim pravima i proaktivne mjere ključni su koraci u očuvanju vaše privatnosti. Budući da je GDPR složena i široka tema, uvijek savjetujemo savjetovanje sa stručnjakom ili nadležnom agencijom.

Digitalni sadržaji o temi mjeseca

Donosimo vam sadržaje koje možete preuzeti i slobodno koristiti za vaše daljnje upoznavanje s temom mjeseca ili za predstavljanje teme u vašem radnom ili privatnom okruženju.

Digitalni tragovi (infografika)	Savjeti za zaštitu na internetu
Digitalni tragovi (prezentacija)	AZOP-ovi vodiči i promotivni materijali
Dobra lozinka	OLIVIA – virtualna asistentica za usklađivanje s GDPR-om

Statistika obrađenih incidenata – prosinac 2024.

Prema dostupnim statistikama Nacionalnog CERT-a za prosinac 2024. godine vidljivo je kako je najveći broj prijavljenih i obrađenih incidenata u kategoriji phishinga što pokazuje kako i dalje postoje brojne kampanje koje ciljaju građane s ciljem prevare i krađe podataka. Više o phishingu.

Phishing	52	42%
Phishing URL	23	19%
Spam	18	15%
Pogađanje zaporki	16	13%
Scam	9	7%
Poslovna prijevara	2	2%
DoS - Volumetrički napad	1	1%
Ostalo	1	1%
Pokušaj iskorištavanja ranjivosti	1	1%
Zavaravanje korisnika	1	1%
Ukupno	124	

Intervju mjeseca

Kako biste opisali trenutnu situaciju u području zaštite osobnih podataka u Hrvatskoj i EU? Koji su najvažniji izazovi s kojima se suočavamo danas?

Zakonska zaštita osobnih podataka u Republici Hrvatskoj u suvremenom smislu, uz postojanje neovisnog nadzornog tijela, ušla je u treće desetljeće obzirom da je prvi Zakon o zaštiti osobnih podataka usvojen već davne 2003. godine, kada je osnovana i Agencija za zaštitu osobnih podataka. Kako se približavamo devetoj obljetnici stupanja na snagu Opće uredbe o zaštiti podataka (OUZP), kao i sedmoj obljetnici njene primjene, ne možemo biti u potpunosti zadovoljni postignutim stupnjem zaštite, ali i razumijevanja ovog u Europskoj uniji temeljnog prava koje pojedinci uživaju sukladno Povelji o temeljnim pravima EU.

Iako su vidljivi pomaci iz perspektive razumijevanja obveza za voditelje i izvršitelje obrade, nažalost još uvijek kao društvo nedovoljno razumijemo, štitimo i ostvarujemo prava koja kao ispitanici imamo u pogledu obrada koje provode voditelji obrade iz javnog i privatnog sektora. Istovremeno, sve šira upotreba tehnologija nadzora i strojnog učenja istovremeno podiže razinu rizika od zloupotrebe naših osobnih podataka, kao i povrede privatnosti općenito.

GDPR (Opća uredba o zaštiti podataka, OUZP) značajno je promijenila pristup zaštiti osobnih podataka. Koji su najveći pomaci u praksi, a što još uvijek predstavlja izazov za organizacije?

To bi svakako bili daljnja razrada modela odgovornosti koji se u europskom zakonodavstvu sustavno razvija od prvih propisa o zaštiti podataka šezdesetih i sedamdesetih godina prošlog stoljeća, zatim Konvencije 108 Vijeća Europe i kasnijih propisa Europske unije (Direktive 95/46 i OUZP), eksplicitno uređenje prava ispitanika

i obveza voditelja obrade kao i detaljnije reguliranje instituta kao što su službenik za zaštitu podataka (DPO), procjena učinka na zaštitu podataka (DPIA).

Uredba je detaljnije regulirala obveze voditelja i izvršitelja obrade, a model upravnih novčanih kazni alternativnog načina izricanja (u apsolutnom novčanom iznosu i u odnosu na ukupan promet organizacije, koji je iznos viši) koristi se i u brojnim drugim suvremenim europskim propisima kao što su Direktiva NIS2, Aktima o umjetnoj inteligenciji (AI Act), o digitalnim uslugama (Digital Services Act), digitalnim tržištima (Digital Markets Act) itd.

Obzirom na ubrzan napredak informacijskih tehnologija, poput umjetne inteligencije, hoće li se i kako pravni okvir prilagođavati kako bi odgovorio na nove prijetnje za privatnost korisnika?

Ovo je odlično pitanje. Uz odgovor prilažem zgodan materijal – jednu infografiku dostupnu na adresi: https://www.bruegel.org/system/files/2024-06/Bruegel_factsheet_2024_0.pdf koja ilustrira razmjere europske zakonodavne aktivnosti na području regulacije zajedničkog digitalnog tržišta.

Iz infografike je vidljivo – europski je zakonodavac iznimno aktivan. Regulacija zaštite temeljnih prava u kontekstu razvoja zajedničkog digitalnog tržišta je u fokusu čitavo desetljeće, i zaštita podataka je samo jedno od područja aktivnosti, u koje se ubrajaju i regulacija kibernetičke sigurnosti i otpornosti, zaštite potrošača, tržišnog natjecanja i digitalnih platformi, pristupa podacima i ponovne upotrebe podataka. Unija je i komparativno gledano vodeća svjetska jurisdikcija po pitanju sustavnog reguliranja izazova tehnologija strojnog učenja, odnosno kako se to danas voli nazivati – umjetne inteligencije.

U tom kontekstu, treba naglasiti da usporedo s važnošću odredbi Uredbe o umjetnoj inteligenciji (AI Act) koja je već djelomično u primjeni, primjenjive odredbe Opće uredbe o zaštiti podataka kad je riječ o obradi osobnih podataka u svrhe povezane s treniranjem i korištenjem sustava umjetne inteligencije su i dalje na snazi. Voditelji obrade koji razvijaju ili koriste rješenja umjetne inteligencije i dalje trebaju voditi računa o načelima zaštite podataka, osobito zakonitosti, transparentnosti i poštenosti, ograničenju svrhe, ograničenju pohrane, kao i općenito obvezama koje propisuje Opća uredba o zaštiti podataka.

Koji su najčešći propusti koje organizacije čine u implementaciji zaštite podataka?

Zahvaljujući javno dostupnim odlukama nacionalnih nadzornih tijela kao i judikaturi sudova država članica Unije, kao i Suda Europske unije, imamo dobar uvid u praksu nadzornih tijela i u statistiku utvrđenih nepravilnosti svih država članica Unije.

Žalosti kako je i dalje vodeći uzrok povreda osobnih podataka obrada podataka bez odgovarajuće pravne osnove, povreda obveza o informiranju ispitanika i druge povrede prava ispitanika, kao i pogreške u odabiru odgovarajućih tehničkih i organizacijskih mjera.

U okviru istraživanja kompetencija i stavova hrvatskih službenika za zaštitu osobnih podataka provedenom neposredno prije službene aktivnosti (tzv. enforcement action) koju je Europski odbor za zaštitu podataka u suradnji s nadzornim tijelima država članica proveo 2023. godine rezultati su pokazali kako službenici za zaštitu osobnih podataka imenovani u hrvatskim organizacijama javnog i privatnog sektora imaju velikih poteškoća s razumijevanjem obveza iz područja zaštite osobnih podataka.

Mnogi od njih nemaju adekvatne resurse i nisu u mogućnosti ispunjavati zadatke propisane Uredbom, osobito u javnom sektoru, a neki nisu upoznati niti s osnovama zaštite osobnih podataka, unatoč obilju izvrsnih resursa dostupnih na stranicama europskih tijela sasvim besplatno, kao što je npr. Priručnik o zaštiti osobnih podataka koji su zajednički pripremili Vijeće Europe i EU Agencija za temeljna prava, a čiji hrvatski prijevod vaši čitatelji mogu sasvim besplatno preuzeti na sljedećoj adresi: https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_hr.pdf

Kako bismo dali svoj doprinos edukaciji službenika za zaštitu podataka, pri Pravnom fakultetu Sveučilišta u Zagrebu pokrenut je program cjeloživotnog obrazovanja kojeg je od 2019. godine pohađalo više od dvije stotine polaznika, u okviru kojeg se polaznici upoznaju s obvezama iz područja zaštite osobnih podataka prema izvorima iz najbolje europske i domaće prakse.

Povodom Dana zaštite osobnih podataka, koje konkretne savjete biste dali građanima u pogledu zaštite vlastitih podataka u svakodnevnom životu, posebno u kontekstu online sigurnosti?

Upoznajte i ostvarujte svoja prava u pogledu zaštite osobnih podataka. Informirani građani koji znaju svoja prava i inzistiraju na njihovoj zaštiti, kako prema voditeljima obrade, tako i prema nadležnom nadzornom tijelu (a u Republici Hrvatskoj to je Agencija za zaštitu osobnih podataka, www.azop.hr) sastavni su element sustava nadzora zaštite osobnih podataka. Pažljivo pročitajte informacije o obradi osobnih podataka prije sklapanja ugovora i davanja osobnih podataka. Obratite se službenicima za zaštitu osobnih podataka oko ostvarivanja svojih prava.

Iako trenutnim stanjem ne možemo biti zadovoljni, ipak naglašavam da je europski pravni i institucionalni okvir zaštite osobnih podataka komparativno uvjerljivo najsnažniji i najučinkovitiji na svijetu, o čemu svjedoče ne samo brojne izrečene kazne i druge mjere, već i opipljiva promjena stavova čak i najvećih divova tehnološke industrije.

Vjerujem da danas niti jedan član ili članica uprave domaće banke ili osiguravajućeg društva više neće za medije izjaviti da će radije plaćati kazne nego se uskladiti s OUZP ili da su troškovi zaštite prava ispitanika od povrede osobnih podataka novac koji bi bilo bolje potrošiti na nešto drugo, kao što se moglo čuti u godinama prije početka primjene OUZP.

Također, sličnu razinu odgovornosti građani s pravom očekuju i od javnih tijela, osobito onih koje obrađuju veliku količinu posebnih kategorija osobnih podataka, kao što su primjerice podaci o zdravlju.

U svijetu tzv. "surveillance kapitalizma" (kako ga naziva američka profesorica Shoshanna Zuboff s Harvard Business School i poznatog Berkman Klein centra za Internet i društvo), gdje osobni podaci postaju nova nafta ili novo zlato, u vječitoj trci za njihovom monetizacijom odnosno komercijalnom eksploatacijom, Europa ostaje svjetionik slobode i visoke ostvarene razine zaštite ljudskih i građanskih prava.

Svim vašim čitateljima i pratiteljima, želim sretan (i informiran) europski Dan zaštite osobnih podataka!

Izv.prof.dr.sc. Tihomir Katulić

Profesor pravnih znanosti na Katedri za pravo informacijskih tehnologija i informatiku Pravnog fakulteta Sveučilišta u Zagrebu. Član International Association of Privacy Professionals - supredsjednik hrvatskog chaptera IAPP KnowledgeNeta i član Global Education Boarda IAPP. Ekspert Europskog odbora za zaštitu podataka (EDPB) External Pool of Experts, EU Cybernet ekspertne grupe, ISO 27001 i 37001 lead auditor. Predsjednik Vijeća stručnjaka Državnog zavoda za intelektualno vlasništvo, voditelj i predsjednik programskog odbora konferencije MIPRO ICTLAW, stalni predavač ljetne škole Svjetske organizacije za intelektualno vlasništvo (WIPO), organizator i stalni predavač programa cjeloživotnog obrazovanja iz zaštite osobnih podataka pri Pravnom fakultetu sveučilišta u Zagrebu. Član hrvatskog Internet Governance Foruma, Hrvatskog društva za autorsko pravo HDAP ALAI i Hrvatskog društva za transportno pravo.

Najava događanja

11. 2. 2025. – Dan sigurnijeg interneta

Povodom Dana sigurnijeg interneta, HAKOM, Udruga Suradnici u učenju, Centar za Sigurniji Internet i CARNET-ov Sektor – Nacionalni CERT, organiziraju konferenciju „Potraga za boljim internetom". Za više informacije o konferenciji pratite obavijesti na našem portalu CERT.hr.

20. 2. 2025. – ConCERT

Druga ConCERT konferencija, u organizaciji CARNET-ovog Nacionalnog CERT-a okupit će stručnjake iz područja kibernetičke sigurnosti kako bi raspravili aktualne teme i događanja. Više informacija pronađite na službenoj stranici konferencije con.cert.hr.