azop
Agencija za zaštitu osobnih podataka

Co-funded by the Rights, Equality and Citizenship Programme of the European Union (2014-2020)

ARC
Awareness raising campaign for SMEs

Zaštita osobnih podataka i usklađivanje s GDPR-om u marketingu

Iva Ivanković, AZOP
Natalija Parlov Una, TÜV NORD

Zagreb, 12. svibnja 2021.

azop
Agencija za zaštitu osobnih podataka

Co-funded by the Rights, Equality and Citizenship Programme of the European Union (2014-2020)

ARC
Awareness raising campaign for SMEs

Opća uredba o zaštiti podataka – GDPR –

ključni pojmovi i pojašnjavanje uloga i odgovornosti voditelja i izvršitelja obrade

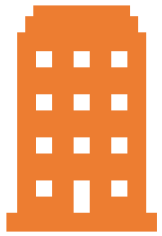
Co-funded by the Rights, Equality and Citizenship Programme of the European Union (2014-2020)

Pravni okvir za marketinšku djelatnost i zaštitu osobnih podataka?

- Opća uredba o zaštiti podataka - GDPR
- Zakon o provedbi Opće uredbe o zaštiti podataka
- Direktiva o privatnosti i elektroničkim komunikacijama
- Zakon o elektroničkim komunikacijama
- Zakon o elektroničkoj trgovini
- Zakon o obveznim odnosima
- Zakon o zaštiti potrošača
- Zakon o nedopuštenom oglašavanju

Izvor: Canva

Opći pojmovi

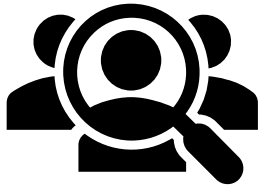


VODITELJ OBRADE (pr. Marketinška agencija, a ne odjel marketinške agencije koji planira obrađivati podatke u svrhe istraživanja tržišta)

Poslovni subjekt koji određuje svrhe i sredstva obrade osobnih podataka

IZVRŠITELJ OBRADE (pr. društvo XX specijalizirano za pohranu podataka u oblaku koje upravlja podacima o kupcima voditelja obrade)

Poslovni subjekt koji obrađuje osobne podatke u ime voditelja obrade i prema uputama
* Ugovor o obradi osobnih podataka

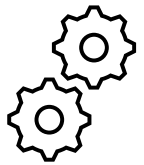


ISPITANIK (pr. kupac, pretplatnik na newsletter, posjetitelj web stranice, zaposlenik)

pojedinac čiji se identitet može utvrditi izravno ili neizravno

OSOBNI PODATAK (pr. ime/prezime, spol, podaci o zdravlju, podatak o lokaciji)

svaki podatak koji se odnosi na pojedinca čiji je identitet utvrđen ili se može utvrditi, a pojedinac čiji se identitet može utvrditi jest osoba koja se može identificirati izravno ili neizravno



OBRADA svaki postupak koji se obavlja na osobnim podacima **(pr. prikupljanje, bilježenje, pohrana, izmjena, obavljanje uvida, uporaba, otkrivanje prijenosom, brisanje ….)**

Co-funded by the Rights, Equality and Citizenship Programme of the European Union (2014-2020)

Načela obrade osobnih podataka

(pouzdanost voditelja obrade)

Načelo zakonitosti, poštenosti i transparentnosti

Načelo ograničavanja svrhe **Primjerice, obrada podataka o kupcima-u svrhu upravljanja odnosima s kupcima (CMR)**

USKLAĐENA SVRHA - statistička analiza ponašanja vlastitih kupaca prilikom kupovnine, **NEUSKLAĐENA SVRHA-** prenošenje podataka drugom društvu koji se bavi izravnim marketingom, a koji želi te podatke iskoristiti kao pomoć u marketinškim kampanjama trećih društava

Načelo smanjenja količine podataka

Načelo točnosti

Načelo ograničenja pohrane

(primjerice, čuvanje videonadzornih snimki max 6 mjeseci)

Načelo cjelovitosti i povjerljivosti

Co-funded by the Rights, Equality and Citizenship Programme of the European Union (2014-2020)

Pravni temelji za obradu osobnih podataka

ispitanik je dao **privolu** za obradu svojih osobnih podataka

(primjerce, privola za analitičke kolačiće, čl. 100 st. 4. ZEK, slanje promidžbene e-pošte)

nužno **za izvršavanje ugovora** u kojem je ispitanik stranka ili kako bi se poduzele radnje na zahtjev ispitanika prije sklapanja ugovora (primjerice, kupoprodaja putem webshop-a)

obrada je nužna radi **poštovanja pravnih obveza** voditelja obrade

(primjerice, davatelj usluga informacijskog društva mora na temelju odgovarajućeg sudskog akta, odnosno upravnog akta, predočiti sve podatke na temelju kojih se može poduzeti otkrivanje ili progon počinitelja kaznenih djela, odnosno zaštita prava trećih osoba.)

obrada je nužna kako bi se zaštitili **životno važni interesi ispitanika** ili druge fizičke osobe

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 (primjerice, slanje promidžbene e-pošte prijašnjim kupcima i dr.)

* obrada je nužna za izvršavanje **zadaće od javnog interesa ili pri izvršavanju službene ovlasti** voditelja obrade

Co-funded by the Rights, Equality and Citizenship Programme of the European Union (2014-2020)

Posebne kategorije podataka

Obrada posebnih kategorija je načelno **zabranjena**.

- **rasno ili etničko podrijetlo,**
- **politička mišljenja,**
- **vjerska ili filozofska uvjerenja ili članstvo u sindikatu**
- **obrada genetskih podataka, biometrijskih podataka u svrhu jedinstvene identifikacije pojedinca**
- **podaci o zdravlju (primjerice, u sklopu programa vjernosti prikupljate podatke o zdravlju) spolnom životu ili seksualnoj orijentaciji pojedinca**

Dopuštena je jedino ako uz postojanje jednog od pravnih temelja za zakonitost obrade iz članka 6. stavka 1. GDPR-a, **postoji i jedna od taksativno navedenih iznimaka iz članka 9. stavka 2. GDPR**.

Legitimni interes

Primjeri obrada koje se mogu temeljiti na legitimnom interesu:

- izravni marketing i drugi oblici marketinga ili oglašavanja
- Videonadzor

! Provjeriti jesu li interesi ispitanika ili njihova temeljna prava jača u odnosu na naš legitimni interes – provođenjem testa ravnoteže

https://azop.hr/obrasci-predlosci/

- Prigovor

Direktni marketing

Marketing usmjeren na određene **pojedince**.
(npr. Pozivi, sms-ovi, e-poruke usmjerene prema nekome)

Što nije direktni marketing?

- Istinsko istraživanje tržišta ne računa se kao izravni marketing. Međutim, ako anketa uključuje bilo koji promotivni materijal ili prikuplja detalje za upotrebu u budućim marketinškim kampanjama, anketa je namijenjena izravnom marketingu.
- Rutinske poruke korisničke službe ne računaju se kao izravni marketing - drugim riječima, prepiska s kupcima radi pružanja informacija koje su im potrebne o trenutnom ugovoru ili prošloj kupnji (npr. informacije o prekidima usluge, aranžmanima isporuke, sigurnosti proizvoda, promjenama uvjeta).
- Općenito brendiranje, logotipi ili trake u ovim porukama ne računaju se kao marketing. Međutim, ako poruka uključuje bilo kakav značajan promotivni materijal usmjeren na kupce da kupe dodatne proizvode ili usluge ili obnove ugovore koji se završavaju, ta poruka uključuje marketinški materijal i primjenjuju se pravila.

Co-funded by the Rights, Equality and Citizenship Programme of the European Union (2014-2020)

Direktni marketing

Upisom u Hakom Registar „Ne zovi” sukladno Pravilniku o registru „Ne zovi“ (NN 47/2016) obrada kontakt podatka ispitanika upisanog u isti postaje nezakonita od strane voditelja/izvršitelja obrade

Dužnost poštivanja zabrane pozivanja brojeva upisanih u registar

Izvor: Canva

Privola

Dobrovoljna – može se povući (pravo na brisanje) i nije uvjetovana*

Posebna – određena svrha

Informirana – voditelj obrade + svrha + …

nedvosmisleno izražavanje želja ispitanika – izjava ili jasna potvrdna radnja

*odbijanje/povlačenje privole ne smije prouzročiti štetne posljedice

+ dokaziva

Izvor: Canva

Savjet!

Vodite evidenciju na što je osoba pristala, te kada i kako ste dobili taj pristanak, kako biste mogli dokazati poštivanje zahtjeva u slučaju nadzora.

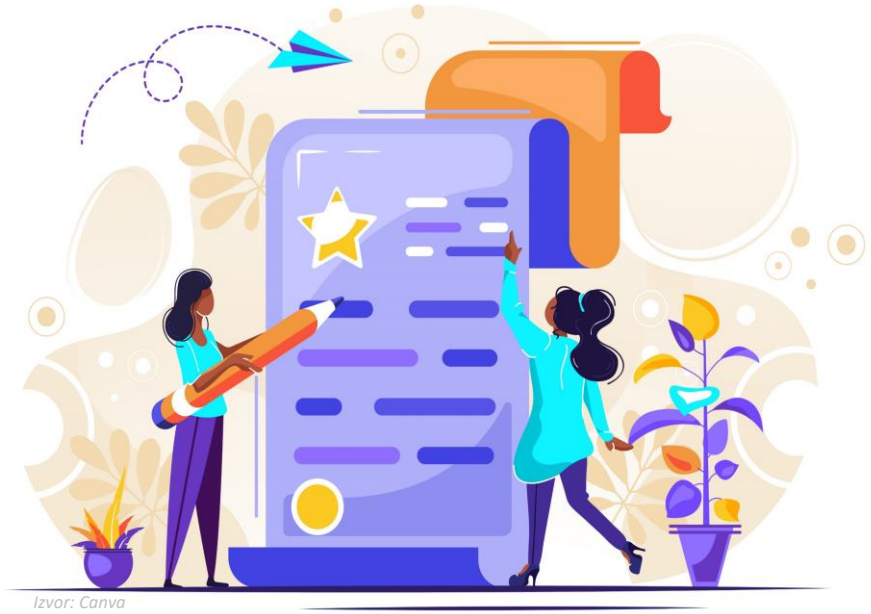
https://azop.hr/obrasci-predlosci/

Co-funded by the Rights, Equality and Citizenship Programme of the European Union (2014-2020)

Prava ispitanika

- pravo na informacije o obradi
- pravo na pristup osobnim podacima koji se odnose na ispitanika
- pravo na prenosivost podataka
- pravo na ispravak — Davatelj usluga informacijskog društva koji podatke, što ih je unio korisnik, priopćava putem komunikacijske mreže nije odgovoran za privremenu pohranu (caching) ako između ostalog: – postupa u skladu s pravilima za ažuriranje podataka
- pravo na brisanje
- pravo na ograničenje obrade
- pravo na prigovor
- pravo prigovoriti na automatiziranom pojedinačnom donošenju odluka, uključujući izradu profila, a koje proizvode pravne učinke

Co-funded by the Rights, Equality and Citizenship Programme of the European Union (2014-2020)



Izvor: Canva

Kako dokazati usklađenost…

Interni akti, evidencije aktivnosti obrade, službenik za zaštitu podataka…

Co-funded by the Rights, Equality and Citizenship Programme of the European Union (2014-2020)

Evidencija aktivnosti obrade

- **zaposleno više od 250 osoba**
  - za sve postupke obrade

- **zaposleno manje od 250 osoba**
  - prouzročiti visok rizik za prava i slobode ispitanika
  - obrada nije povremena
  - obrada uključuje posebne kategorije
  - osobnim podacima u vezi s kaznenim osudama i kažnjivim djelima

Voditelj obrade:	A d.o.o.	
Kategorija ispitanika i osobnih podataka:	Videozapis posjetitelja objekta na adresi _____	
Svrha:	zaštita osoba i imovine	
Primatelji: B d.o.o. **Prijenos: -**	**Rok za brisanje:** 6 mjeseci	**Teh. i org. mjere:** Interni akti, edukacija

Izvršitelj obrade: B d.o.o.	**Voditelj obrade:** A d.o.o.
Vrsta obrade: videonadzor u svrhu zaštite osoba i imovine objekta na adresi _____	
Prijenos: -	**Teh. i org. Mjere:** izjave o povjerljivosti, politike informacijske sigurnosti, edukacije zaposlenika…

Voditelj/izvršitelj obrade

01

izvršitelj obrađuje osobne podatke samo **prema zabilježenim uputama voditelja** obrade

02

izvršitelj osigurava da su se **osobe ovlaštene za obradu osobnih podataka obvezale na poštovanje povjerljivosti**

03

izvršitelj poduzima **sve potrebne tehničke i organizacijske mjere**

04

izvršitelj **ne smije angažirati drugog izvršitelja obrade** bez prethodnog posebnog ili općeg pisanog odobrenja voditelja obrade

Voditelj/izvršitelj obrade

05

izvršitelj pomaže u osiguravanju usklađenosti

06

po izboru voditelja, briše ili vraća voditelju obrade sve osobne podatke nakon dovršetka pružanja usluga

07

pomaže s dokazivanjem usklađenosti s GDPR-om (za revizije, inspekcije,…)

Povreda osobnih podataka

kršenje sigurnosti koje dovodi do slučajnog ili nezakonitog uništenja, gubitka, izmjene, neovlaštenog otkrivanja ili pristupa osobnim podacima

a. Izvješće nadzornom tijelu

- ako postoji **rizik** za prava i slobode pojedinaca
- unutar 72 sata od saznanja

b. Obavješćivanje ispitanika o povredi osobnih podataka

- ako postoji visok rizik za prava i slobode pojedinaca

c. Sadržaj izvješća:

- (a)opis povrede
- (b)podatke službenika za zaštitu podataka
- (c)opis vjerojatnih posljedica povrede
- (d)opis mjera poduzetih za rješavanje problema povrede

Kada nije obvezno obavijestiti ispitanika?
(a) primijenjene tehničke i organizacijske mjere zaštite pr. enkripcija
(b) voditelj obrade poduzeo je naknadne mjere kojima se osigurava da više nije vjerojatno da će doći do visokog rizika
(c) time bi se zahtijevao nerazmjeran napor – pr. javno obavješćivanje

Izvršitelj obrade izvješćuje voditelja obrade!!!!!

Co-funded by the Rights, Equality and Citizenship Programme of the European Union (2014-2020)

Posljedice za pojedinca radi povrede osobnih podataka!

krađa identiteta ili prijevara

Povreda dostojanstva

Imovinska/neimovinska šteta

Procjena učinka na zaštitu osobnih podataka

ZAŠTO se provodi?

Kako bi znali koje teh. i org. mjere treba primijeniti na **visokorizičnu obradu**

- Primjer obrasca možete pronaći na https://azop.hr/obrasci-predlosci/

- **KOJA obrada je visokorizična?**
  - popis možete pronaći na www.azop.hr
  - ako obrada ispunjava dva kriterija od devet kriterija*

- **KAKO provesti procjenu učinka?**

  - opis postupaka obrade i svrha obrade
  - procjenu nužnosti i proporcionalnosti u odnosu na svrhu
  - procjenu rizika za prava i slobode ispitanika
  - mjere predviđene za rješavanje problema rizika

Co-funded by the Rights, Equality and Citizenship Programme of the European Union (2014-2020)

Službenik za zaštitu osobnih podataka

Imate li imenovanog službenika za zaštitu podataka?

Ako da, zašto je važan?

temelj pouzdanosti, posrednik, konkurentska prednost

Ako ne, postoji li obveza?

članak 37. GDPR, osnovna djelatnost

Kakav bi službenik trebao biti?

neovisan, stručan, ne u sukobu interesa

Položaj i zadaće?

Resursi za rad, upute, odgovornost

Koja se pravila primjenjuju na međunarodne marketinške kampanje?

Unutar EEA?

Ako šaljete poruke zemljama izvan RH, također se morate pridržavati njihovih zakona.
Trenutno države EU imaju vrlo slične propise kao i oni koji se temelje na Direktivi o e-privatnosti.

Izvan EEA?

Primjerice, o slanju i analitici uspješnosti newslettera se brine društvo iz Srbije ili Bosne i Hercegovine

Primjena poglavlja V. GDPR-a (zaštitne mjere)

Što pripremiti za nadzor?

- Evidencije aktivnosti obrade
- Interne akte kojima je regulirana zaštita osobnih podataka
  (npr. Politika privatnosti, interni akti koji uređuju informacijsku sigurnost, videonadzorni sustav)
- Ugovor sa Izvršiteljem obrade
- Izjave o povjerljivosti
- Dokumentacija odnosna na predmetni slučaj i ispitanika/e

Co-funded by the Rights, Equality and Citizenship Programme of the European Union (2014-2020)

Specifičnosti obrade osobnih podataka u marketingu

Co-funded by the Rights, Equality and Citizenship Programme of the European Union (2014-2020)

Cvjećarnica *Jorgovan*

Studija slučaja / Case study

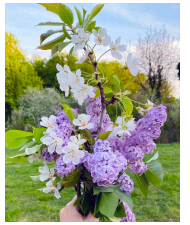
NPARL v1.0_10052021

Studija slučaja – Cvjećarnica Jorgovan

- Cvjećarnica prodaje cvjetne aranžmane na
  (1) **fizičkim prodajnim mjestima** i putem (2) **webshopa**
- Aktivno koristi društvene mreže i ima službene profile na Facebook-u i Instagramu putem kojih ponekad organizira nagradne natječaje s odličnim odazivom.
- Prije prve kupnje u prodavaonici ili prilikom registracije u webshop, kupcima se nudi učlanjenje u program vjernosti (*loyalty*) gdje skupljanjem bodova ostvaruju popuste na buduće kupnje i informira ih se o akcijama i proizvodima koji bi ih mogli zanimati putem *newslettera*.
- Kupci cvjetne aranžmane za različite prigode mogu i unaprijed naručiti telefonom ili online, a preuzeti ih mogu osobno ili im se šalju dostavnom službom.
- U organizaciji poslovanja tvrtka koristi interni CRM sustav te poznati knjigovodstveni program.
- Poslovni prostori su u zakupu, a za zaštitu pojedinih poslovnica od provala koristi se videonadzor sa sustavom pohrane koji je u njenom vlasništvu.

Studija slučaja - Cvjećarnica Jorgovan

Kako znamo gdje su osobni podaci?



- **Cvjećarnica** prodaje cvjetne aranžmane na (1) **fizičkim prodajnim mjestima** i putem (2) **webshopa**
- Aktivno koristi društvene mreže i ima službene profile na Facebook-u i Instagramu putem kojih ponekad organizira nagradne natječaje s odličnim odazivom.
- Prije prve kupnje u prodavaonici ili prilikom registracije u webshop, kupcima se nudi učlanjenje u program vjernosti (*loyalty*) gdje skupljanjem bodova ostvaruju popuste na buduće kupnje i informira ih se o akcijama i proizvodima koji bi ih mogli zanimati putem *newslettera*.
- Kupci cvjetne aranžmane za različite prigode mogu i unaprijed naručiti telefonom ili online, a preuzeti ih mogu osobno ili im se šalju dostavnom službom.
- U organizaciji poslovanja tvrtka koristi interni CRM sustav te poznati knjigovodstveni program.
- Poslovni prostori su u zakupu, a za zaštitu pojedinih poslovnica od provala koristi se videonadzor u glavnoj prostoriji sa sustavom pohrane koji je u njenom vlasništvu.

Studija slučaja - Cvjećarnica Jorgovan

Odakle početi?

- **Cvjećarnica** prodaje cvjetne aranžmane na
  (1) **fizičkim prodajnim mjestima** i putem (2) **webshopa**

- **Makro pogled:**
  - **Osobni podaci:** uprava, zaposlenici, dobavljači, najmodavci, kupci, potencijalni kupci (loyalty, akcije, socnet) …
  - **Pravna osnova:** zakonska osnova, ispunjenje ugovorne obveze, legitimni interes, privola
  - **Status trećih strana vezanih uz procesiranje OP:** zajednički voditelji obrada i izvršitelji obrada

Studija slučaja - Cvjećarnica Jorgovan

Prikupljanje osobnih podataka na fizičkoj lokaciji

Cvjećarnica ima fizička prodajna mjesta gdje kupci mogu:

- Doći i kupiti proizvode.
- Učlaniti se u program vjernosti čak i bez kupnje.
- Ostvariti pogodnosti i popuste *voucherima* ili unovčavanjem bodova.
- Naručiti proizvode po narudžbi putem telefona i preuzeti ih na lokaciji.
- Osobno preuzeti proizvode koje su prethodno platili putem webshopa.

Videonadzor na pojedinim fizičkim prodajnim mjestima služi isključivo u svrhu zaštite od provala.

Studija slučaja - Cvjećarnica Jorgovan

Prikupljanje putem internetske stranice

Webshop ima registraciju korisnika **koji kupuju** proizvode ali i onih koji su se **registrirali i ne kupuju** nego samo gledaju asortiman ili samo stavljaju u košaricu.

Kupnja se odvija kartičnim plaćanjem ili plaćanjem pouzećem. Po narudžbi ili plaćanju proizvoda karticom kupac na e-mail dobiva potvrdu o narudžbi, načinu i roku dostave te statusu plaćanja.

Webshop ima opcije **prilagođenog prikazivanja vezanih proizvoda** s obzirom na pregledavane ili kupljene proizvode (kupci koji su gledali ovaj proizvod gledali su još i ovaj…)

Studija slučaja - Cvjećarnica Jorgovan

Povezanost različitih servisa i prikupljanje putem društvenih mreža

Cvjećarnica ima otvorene kanale na društvenim mrežama na kojima periodično organizira **nagradne natječaje** i dijeli svoje proizvode kao nagrade.

U marketingu ponekad koristi i usluge **Google Ads** koji su svojim postavkama povezani s webshopom i društvenim mrežama, te koristi i oglašavanje na Facebooku i Instagramu.

Studija slučaja - Cvjećarnica Jorgovan

Program vjernosti (*loyalty*)

Cvjećarnica ima aktivni **program vjernosti** odnosno *loyalty* –
prije prve kupnje potencijalni kupci se upućuju da ispune **fizičku karticu** za klub vjernosti koju im daje blagajnik ili da se na njega **online registriraju** putem webshopa.

Na webshopu kupac ima svoj **profil** na kojem vidi sve kupnje ostvarene putem webshopa te ukupni broj bodova koji je ostvario na bilo kojem od prodajnih mjesta (fizička ili webshop).

Bodove može konzumirati na bilo kojem njenom prodajnom mjestu jer je **program vjernosti povezan** s knjigovodstvenim programom zbog ostvarenja rabata i praćenja stanja na skladištu.

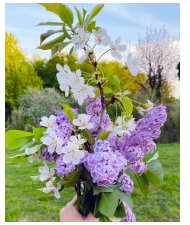
Studija slučaja - Cvjećarnica Jorgovan

Direktni mailing – fizički i digitalni

Program vjernosti prikuplja i podatke o *imenu i prezimenu, adresi za račun i adresi za dostavu, datumu rođenja, spolu i dobi*, te automatiziranim procesom generira *vouchere* s popustom kupcima za njihov rođendan, proizvode koji bi im mogli odgovarati, blagdanskim akcijama i o tome ih informira automatiziranim e-mailom i tiskanim pošiljkama.

Cvjećarnica koristi direktni mailing putem *newsletter* programa na adrese registriranih korisnika webshopa i članova programa vjernosti.

Uz mail, uvijek se tiskaju rođendanski *voucheri* koji se šalju na fizičke adrese kupaca ili personalizirani *voucheri* vezani uz Dan žena i slično jer je primijećeno da imaju značajan utjecaj na povećanje prodaje.



Studija slučaja - Cvjećarnica Jorgovan

Osim zakonom uvjetovanih, s kojim još trećim stranama dijeli osobne podatke?

Cvjećarnica koristi **interni knjigovodstveni program** od dobavljača iz Zagreba, koji je putem API-ja spojen s *webshopom* zbog bodova i stanja na skladištu te **vanjski knjigovodstveni servis** iz Zagreba.

Zakup internetskih stranica (hosting) plaća se na godišnjoj bazi tvrtki iz Rijeke, i serveri su locirani u Hrvatskoj.

Izrada i programiranje te održavanje *webshopa* kontinuirano pruža tvrtka iz Zagreba.

O **planiranju, slanju i analitici uspješnosti *newslettera*** se brine tvrtka iz Srbije.

Organizaciju i provedbu nagradnih natječaja putem društvenih mreža i njihovo održavanje te odgovaranje na upite koji pristižu u *inbox* radi marketinška agencija iz Zagreba.

Tiskara koja tiska **personalizirane *vouchere*** za direktni mailing je iz okolice Zagreba.

Za **dostavu proizvoda** koriste se usluge različitih dostavnih službi.

Za **program vjernosti** koristi se jedan od *plug-inova* dostupnih na Wordpress platformi, plaćena verzija, ali programer trenutno ne zna gdje se nalazi tvrtka koja je vlasnik tog *plug-ina* i pretpostavlja da je s područja SAD-a.

Co-funded by the Rights, Equality and Citizenship Programme of the European Union (2014-2020)

Organizacijske i tehničke mjere u usklađivanju s GDPR-om

Co-funded by the Rights, Equality and Citizenship Programme of the European Union (2014-2020)

Organizacijske i tehničke mjere

ORGANIZACIJSKE MJERE ZAŠTITE

- ✓ odnose se na **dokumentirano uređenje** te **organizacijsku kulturu, poslovnu praksu i procese** unutar subjekta na način da se internim aktima i ugovornim klauzulama uređuje područje zaštite osobnih podataka koje organizacija obrađuje te da se **propisano aktivno procesno provodi** sukladno dokumentiranoj informaciji i da je u mogućnosti **nedvojbeno to dokazati**

TEHNIČKE MJERE ZAŠTITE

- ✓ odnose se na **zaštitne mjere** koje se postavljaju na **fizička mjesta te IT sustave ili proizvode** koji se koriste unutar organizacije ili u sklopu krajnjih proizvoda klijentima, a vezano uz ophođenje s podacima; ili tehničke mjere koje organizacija **ugovorno regulira s trećim stranama** koje imaju uvid ili s kojima sudjeluje u obradi ili pohrani podataka, a da su sve od navedenih strana u mogućnosti **nedvojbeno to dokazati**

ORGANIZACIJSKE MJERE ZAŠTITE

Primjeri internih akata kojima se uređuje područje zaštite osobnih podataka koje poslovni subjekt obrađuje:

- Pravilnik o informacijskoj sigurnosti
- Pravilnici kojima se uređuje obrada pojedinih zbirki podataka *(Pravilnik o videonadzoru, Pravilnik o evidenciji radnog vremena, Politika sigurnog korištenja Interneta, …)*
- Ugovorne klauzule unutar ugovora o radu
- Ugovorne klauzule unutar ugovora o poslovnoj suradnji
- Izjave o povjerljivosti
- …

ORGANIZACIJSKE MJERE ZAŠTITE

EDUKACIJA I PODIZANJE SVIJESTI O VAŽNOSTI ZAŠTITE PODATAKA

- koje sve osobne (ili vrijedne poslovne) podatke zaposlenici koriste i obrađuju u svom svakodnevnom radu
- kojim kategorijama osobnih podataka ti podaci pripadaju
- gdje se ti podaci nalaze
- koji su potencijalni rizici od krađe, zlouporabe i gubitka tih podataka
- na koji način te podatke mogu zaštititi
- kako se to negativno može reflektirati na poslovni subjekt u kojem rade, a u krajnjoj mjeri i na njih same
- da je potrebno svakodnevno se pridržavati preporučenih i propisanih mjera zaštite radi smanjenja potencijalnih rizika od neovlaštenog pristupa i zlouporabe na najmanju moguću mjeru

Analiza rizika

Preventivne i korektivne radnje

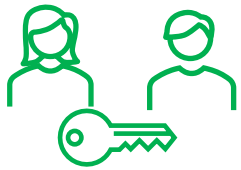
Kontinuirani nadzor i mjerenje

Co-funded by the Rights, Equality and Citizenship Programme of the European Union (2014-2020)

TEHNIČKE MJERE ZAŠTITE

Neovlašteni zaposlenici

Poslovno



Ovlašteni zaposlenici

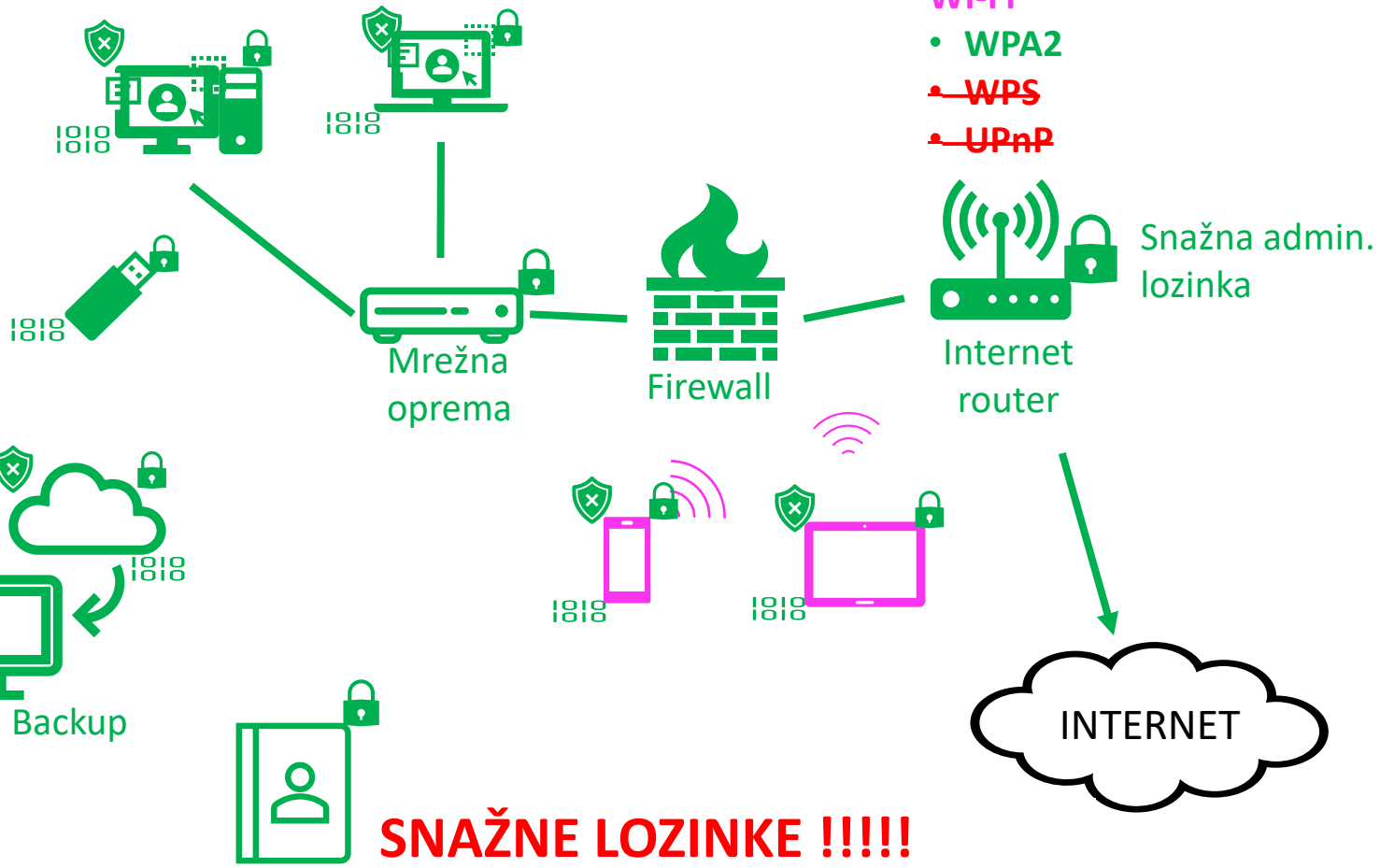
Privatno

Nadograđeni OS i programi

Antivirus

Lozinka Ovlasti

Kriptirani podaci



Postoje li konkretne smjernice?

- Međunarodni ISO standardi koje preporuča Europska Komisija i sadrže **cjelokupne konkretne smjernice** s **detaljno razrađenim tehničkim i organizacijskim mjerama**:

  ISO/IEC 27001 Sustavi upravljanja informacijskom sigurnosti
  ISO/IEC 27701 Sustavi upravljanja informacijama o privatnosti

- Rezultat njihovog **pravilnog uvođenja**:

  ✓ Formirani ili restrukturirani poslovni procesi, ažurirani interni akti, politike informacijske sigurnosti i zaštite osobnih podataka, efikasan sustav preventivnih i korektivnih mjera te internog praćenja i sprječavanja sigurnosnih incidenata

  ✓ Dokazi za audite/revizije, inspekcije i ostale dionike (fizičke osobe čiji podaci se štite, kupce, dobavljače, ostale treće strane)

  ✓ Olakšano usklađivanje s regulativom vezanom uz informacijsku sigurnost i zaštitu osobnih podataka

Co-funded by the Rights, Equality and Citizenship Programme of the European Union (2014-2020)

Usklađivanje internetskih stranica s GDPR-om i kolačići

Politika privatnosti za web

1. identitet i kontaktne podatke voditelja obrade (kontakt službenika za zaštitu podataka)
2. vrste osobnih podataka se obrađuju
3. svrhe obrade radi kojih se upotrebljavaju osobni podaci kao i pravnu osnovu za obradu
4. legitimne interese voditelja obrade ili treće strane;
5. primatelje ili kategorije primatelja osobnih podataka
6. prijenos u treću zemlju ili međunarodnu organizaciju + zaštitne mjere
7. razdoblje pohrane ili, ako to nije moguće, kriterije kojima se utvrdilo to razdoblje
8. prava ispitanika
9. informaciju o tome je li pružanje osobnih podataka zakonska ili ugovorna obveza ili uvjet nužan za sklapanje ugovora te ima li ispitanik obvezu pružanja osobnih podataka i koje su moguće posljedice ako se takvi podaci ne pruže
10. postojanje automatiziranog donošenja odluka/izradu te smislene informacije o tome o kojoj je logici riječ, kao i važnost i predviđene posljedice takve obrade za ispitanika

Savjeti

- Izvršitelja obrade koji vam pruža IT usluge izrade ili održavanja internetskih stranica možete zatražiti analizu korištenih kolačića i popis trećih strana za *plug-inove* koje koristi vaša internetska stranica kako biste mogli provjeriti njihovu usklađenost, osobito ako se radi o funkcijama vezanim uz obrade osobnih podataka ili mogućnosti pristupa njima.
- *Plug-inovi* za automatsko generiranje politika privatnosti uspješni su isključivo ako generirana informacija sadrži potpune podatke koje takav dokument treba sadržavati, te ako su sadržane informacije u skladu sa stvarnim procesima i svrhom za koju su namijenjeni.
- Uputno je da voditelj obrade inicira regulaciju međusobnog ugovornog odnosa s izvršiteljem obrade i **nedvojbeno se uvjeri** u Izvršiteljevu usklađenost s GDPR-om.
- Provjerite gdje (u kojoj zemlji) su smješteni serveri na kojima se nalaze vaše internetske stranice ukoliko putem njih prikupljate osobne podatke ili e-mail računi.

Kolačići *(cookies)*

- Male datoteke koje internetski preglednik pohranjuje na računalo, mobilni uređaj ili drugi uređaj kojim je korisnik posjetio neku internetsku lokaciju.
- Služe za osiguravanje funkcionalnosti, unaprjeđenje korisničkog iskustva, praćenje ponašanja, omogućavanje i olakšavanje pristupa …
- Dijele se prema **trajanju**, **izvoru** i **funkciji**.

Kolačići *(cookies)*

Prema **trajanju** kolačići mogu biti:

- ✓ **Stalni kolačići (spremljeni)** (eng Persistent Cookies)
- ✓ **Privremeni ili sesijski kolačići** (eng. Session Cookies)

Prema **izvoru** kolačići mogu biti:

- ✓ **Kolačići prve strane** (*first-party cookie*)
- ✓ **Kolačići treće strane** (*third-party cookie*)

Prema **funkciji** postoji više vrsta kolačića, a najčešće su:

- ✓ **Tehnički/neophodni kolačići**
- ✓ **Funkcionalni kolačići**
- ✓ **Statistički kolačići**
- ✓ **Marketinški kolačići**

Co-funded by the Rights, Equality and Citizenship Programme of the European Union (2014-2020)

Privola za kolačiće (pop-up)

- ✓ Na terminalnoj opremi korisnika **ne smije biti pohranjen niti jedan kolačić za kojeg je potrebna privola** sve dok korisnik ne da izričitu privolu za pohranu tih kolačića.
- ✓ Privola **ne smije biti uvjetovana**. Korisniku mora biti objašnjeno koji opseg osobnih podataka će se prikupljati i u koju svrhu te mu omogućiti da sam odluči daje li pristanak na obradu tog opsega podataka ili ne.
- ✓ Korisnik privolu treba dati **za svaku vrstu kolačića po njihovoj funkcionalnosti posebno**, odnosno da **ne može biti objedinjena privola za sve vrste kolačića.**

Co-funded by the Rights, Equality and Citizenship Programme of the European Union (2014-2020)

PRIMJERI LOŠE PRAKSE

PRIMJER 1

Ova internetska stranica upotrebljava kolačiće. Prihvaćanje kolačića omogućuje optimalno pregledavanje sadržaja.

Prihvaćam

PRIMJER 2

Kolačiće koristimo kako bismo poboljšali iskustvo korištenja naše stranice. Pritiskom na bilo koju poveznicu na ovoj stranici prihvaćate korištenje kolačića.

OK

PRIMJERI LOŠE PRAKSE

PRIMJER 3

Ove internetske stranice koriste kolačiće (tzv. cookies) za pružanje boljeg korisničkog iskustva i funkcionalnosti. Postavke kolačića možete podesiti u svojem internetskom pregledniku. Više o kolačićima i načinu kako ih koristimo te načinu kako ih onemogućiti pročitajte ovdje.

OK

- Odabirom poveznica o više informacija otvara se novi skočni prozor ili Internet stranica informativnog sadržaja na kojoj su **opisani kolačići koje Internet mjesto koristi i u koju svrhu**, ali korisniku **ne nude mogućnost da odabere skupine kolačića po njihovoj funkcionalnosti (odnosno svrsi) za koje daje privolu**, već ga se upućuje da postavke kolačića može regulirati kroz svoj Internet preglednik, uz eventualnu uputu na kojim mjestima može pronaći daljnje upute kako se kolačići podešavaju u pojedinoj vrsti Internet preglednika.

Co-funded by the Rights, Equality and Citizenship Programme of the European Union (2014-2020)

PRIMJERI LOŠE PRAKSE

Internet mjesto stavlja kolačiće, pristupa općim i neosjetljivim podacima s vašeg uređaja te ih upotrebljava kako bi poboljšalo proizvode Internet mjesta i prilagodilo oglase i druge sadržaje na Internet mjestu. Možete prihvatiti sve ili dio tih postupaka. Kako biste saznali više o kolačićima i načinu na koji Internet mjesto upotrebljava vaše podatke te pregledati svoje mogućnosti posjetite stranicu pravila o zaštiti privatnosti

Primjena istraživanja tržišta radi generiranja uvida u publiku

Ne prihvaćam Prihvaćam

Istraživanje tržišta može se koristiti kako bi se saznalo više o publici koja posjećuje web lokacije / aplikacije i pregledava oglase.

Mjerenje učinkovitosti sadržaja

Ne prihvaćam Prihvaćam

Moguće je mjerenje djelotvornosti i učinkovitosti sadržaja koji vidite ili s kojim vršite interakciju.

Stvaranje profila prilagođenog sadržaja

Ne prihvaćam Prihvaćam

Moguće je načiniti profil o vama i vašim interesima kako bi vam se prikazivali upravo vama prilagođeni sadržaji.

Stvaranje personaliziranog profila oglasa

Ne prihvaćam Prihvaćam

Profil može biti izrađen na temelju vaših interesa kako bi vam se prikazivale vama prilagođeni oglasi koji vas mogu zanimati."

OK

Co-funded by the Rights, Equality and Citizenship Programme of the European Union (2014-2020)

PRIMJERI DOBRE PRAKSE

Internet mjesto stavlja kolačiće, pristupa općim i neosjetljivim podacima s vašeg uređaja te ih upotrebljava kako bi poboljšalo proizvode Internet mjesta i prilagodilo oglase i druge sadržaje na Internet mjestu. Možete prihvatiti sve ili dio tih postupaka. Kako biste saznali više o kolačićima i načinu na koji Internet mjesto upotrebljava vaše podatke te pregledati svoje mogućnosti posjetite stranicu pravila o zaštiti privatnosti

Primjena istraživanja tržišta radi generiranja uvida u publiku

Ne prihvaćam Prihvaćam

Istraživanje tržišta može se koristiti kako bi se saznalo više o publici koja posjećuje web lokacije / aplikacije i pregledava oglase.

Mjerenje učinkovitosti sadržaja

Ne prihvaćam Prihvaćam

Moguće je mjerenje djelotvornosti i učinkovitosti sadržaja koji vidite ili s kojim vršite interakciju.

Stvaranje profila prilagođenog sadržaja

Ne prihvaćam Prihvaćam

Moguće je načiniti profil o vama i vašim interesima kako bi vam se prikazivali upravo vama prilagođeni sadržaji.

Stvaranje personaliziranog profila oglasa

Ne prihvaćam Prihvaćam

Profil može biti izrađen na temelju vaših interesa kako bi vam se prikazivale vama prilagođeni oglasi koji vas mogu zanimati."

OK

PRIMJERI DOBRE PRAKSE

Internet mjesto stavlja kolačiće, pristupa općim i neosjetljivim podacima s vašeg uređaja te ih upotrebljava kako bi poboljšalo proizvode Internet mjesta i prilagodilo oglase i druge sadržaje na Internet mjestu. Možete prihvatiti sve ili dio tih postupaka. Kako biste saznali više o kolačićima i načinu na koji Internet mjesto upotrebljava vaše podatke te pregledati svoje mogućnosti posjetite stranicu pravila o zaštiti privatnosti

Primjena istraživanja tržišta radi generiranja uvida u publiku

Ne prihvaćam | Prihvaćam

Istraživanje tržišta može se koristiti kako bi se saznalo više o publici koja posjećuje web lokacije / aplikacije i pregledava oglase.

Mjerenje učinkovitosti sadržaja

Ne prihvaćam | Prihvaćam

Moguće je mjerenje djelotvornosti i učinkovitosti sadržaja koji vidite ili s kojim vršite interakciju.

Stvaranje profila prilagođenog sadržaja

Ne prihvaćam | Prihvaćam

Moguće je načiniti profil o vama i vašim interesima kako bi vam se prikazivali upravo vama prilagođeni sadržaji.

Stvaranje personaliziranog profila oglasa

Ne prihvaćam | Prihvaćam

Profil može biti izrađen na temelju vaših interesa kako bi vam se prikazivale vama prilagođeni oglasi koji vas mogu zanimati."

Ne prihvaćam sve | Prihvaćam sve | OK

PRIMJERI DOBRE PRAKSE

Internet mjesto stavlja kolačiće, pristupa općim i neosjetljivim podacima s vašeg uređaja te ih upotrebljava kako bi poboljšalo proizvode Internet mjesta i prilagodilo oglase i druge sadržaje na Internet mjestu. Možete prihvatiti sve ili dio tih postupaka. Kako biste saznali više o kolačićima i načinu na koji Internet mjesto upotrebljava vaše podatke te pregledati svoje mogućnosti posjetite stranicu pravila o zaštiti privatnosti

Primjena istraživanja tržišta radi generiranja uvida u publiku

Ne prihvaćam | Prihvaćam

Istraživanje tržišta može se koristiti kako bi se saznalo više o publici koja posjećuje web lokacije / aplikacije i pregledava oglase.

Mjerenje učinkovitosti sadržaja

Ne prihvaćam | Prihvaćam

Moguće je mjerenje djelotvornosti i učinkovitosti sadržaja koji vidite ili s kojim vršite interakciju.

Stvaranje profila prilagođenog sadržaja

Ne prihvaćam | Prihvaćam

Moguće je načiniti profil o vama i vašim interesima kako bi vam se prikazivali upravo vama prilagođeni sadržaji.

Stvaranje personaliziranog profila oglasa

Ne prihvaćam | Prihvaćam

Profil može biti izrađen na temelju vaših interesa kako bi vam se prikazivale vama prilagođeni oglasi koji vas mogu zanimati."

Ne prihvaćam sve | Prihvaćam sve | OK

Često postavljana pitanja

- Koji je najbolji način za sastavljanje vlastite marketinške *mailing* liste?
  Koristite podatke o ljudima koji su u prošlosti kupovali robu/usluge ili koji su se registrirali na Vašem web mjestu/postavili upit. Unaprijed jasno stavite do znanja da namjeravate koristiti njihove podatke u marketinške svrhe. Zabilježite radi li se o kupcu-fizičkoj osobi ili društvu (GDPR ne štiti podatke društva). Vodite računa o pravnom temelju za obradu podataka i svim uvjetima za određeni pravni temelj (privola/l. interes).

- Kako bismo trebali odgovoriti na prigovore ili povlačenja privole?
  Čim netko prigovori Vašem marketingu ili ga onemogući, trebali biste ga dodati na popis "ne kontaktiraj". Trebali biste provjeriti svoje marketinške aktivnosti na ovom popisu kako biste bili sigurni da ne kontaktirate nikoga tko je prigovorio/povukao privolu.

- U slučaju prigovora ili povlačenja privole možemo li poslati poruku u kojoj potvrđujemo da se osoba odjavila/povukla privolu?
  Da, ali ne smijete ih kontaktirati kasnije, čak i ako se radi samo o pitanju žele li se pojedinci ponovno uključiti.

Co-funded by the Rights, Equality and Citizenship Programme of the European Union (2014-2020)

Često postavljana pitanja

- Možemo li slati marketinške poruke poštom?
  Direktiva o e-privatnosti se ne primjenjuje na poštanske usluge, međutim u svakom slučaju morate se pridržavati Opće uredbe o zaštiti podataka i Zakona o provedbi Opće uredbe o zaštiti podataka te odredbi Zakona o zaštiti potrošača koji određuje kako je zabranjeno je ostavljanje oglasnih poruka i materijala u ili na poštanskim sandučićima te na ili ispred kućnih vrata potrošača ako je takva zabrana na njima jasno napisana.

- Moramo li potpuno izbrisati kontakte osoba koje su se odjavile (prigovorile) ili povukle privolu?
  Ne, u slučaju zahtjeva za brisanjem podataka objasnite im da ćete ih morati zadržati na popisu "ne kontaktiraj" kako biste bili sigurni da se pridržavate njihovog prava.

- Što trebamo učiniti kako bismo se pridržavali pravila u vezi kolačića?
  Objasnite pojedincima da koristite kolačiće, što kolačići rade i zašto te omogućite pojedincima da vam daju privolu. Ako se Vaša uporaba kolačića s vremenom promijeni zatražite privolu ispočetka.

Co-funded by the Rights, Equality and Citizenship Programme of the European Union (2014-2020)

PITANJA?

Agencija za zaštitu osobnih podataka
www.azop.hr
www.arc-rec-project.eu/
info@arc-rec-project.eu