GDPR

dr.sc. Daniel Bara

16.12.2024


General
Data
Protection
Regulation

UREDBA (EU) 2016/679 EUROPSKOG PARLAMENTA I VIJEĆA

od 27. travnja 2016.

o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka)

Zašto GDPR?

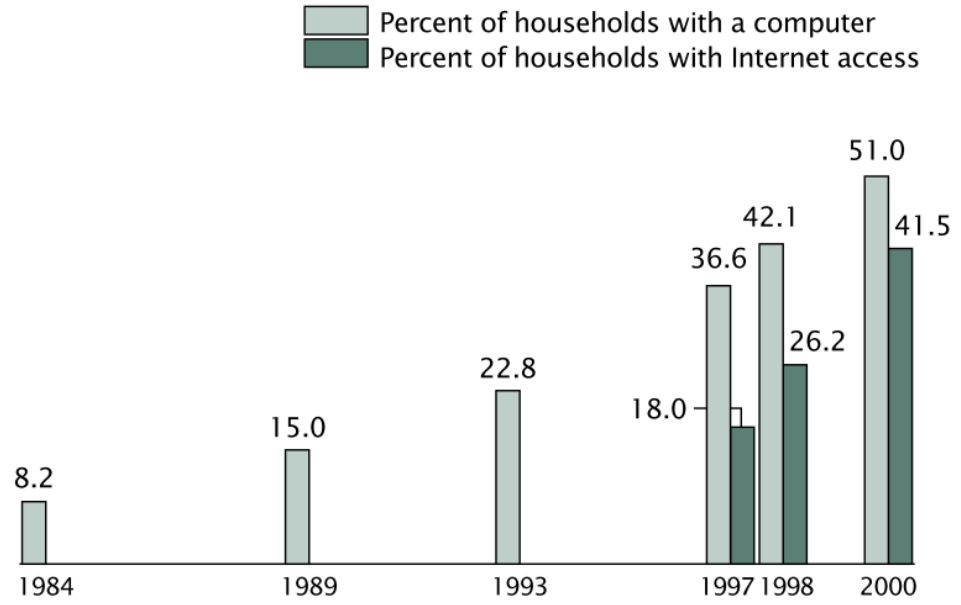
- Zaštita pojedinaca s obzirom na obradu osobnih podataka temeljno je pravo.
- Člankom 8. stavkom 1. Povelje Europske unije o temeljnim pravima („Povelja”) te člankom 16. stavkom 1. Ugovora o funkcioniranju Europske unije (UFEU) utvrđuje se da *svatko ima pravo na zaštitu svojih osobnih podataka*.

Zašto GDPR?

Figure 1.

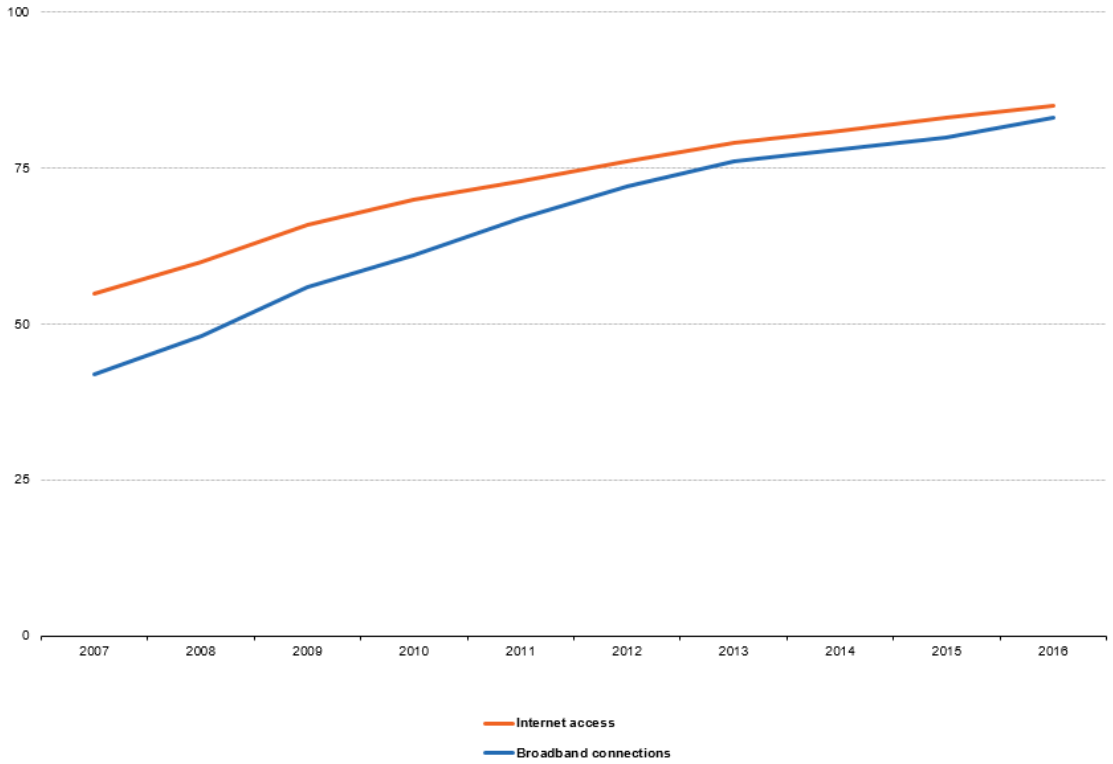
Computers and Internet Access in the Home: 1984 to 2000

(Civilian noninstitutional population)



Note: Data on Internet access were not collected before 1997.
Source: U.S. Census Bureau, Current Population Survey, various years.

Zašto GDPR?



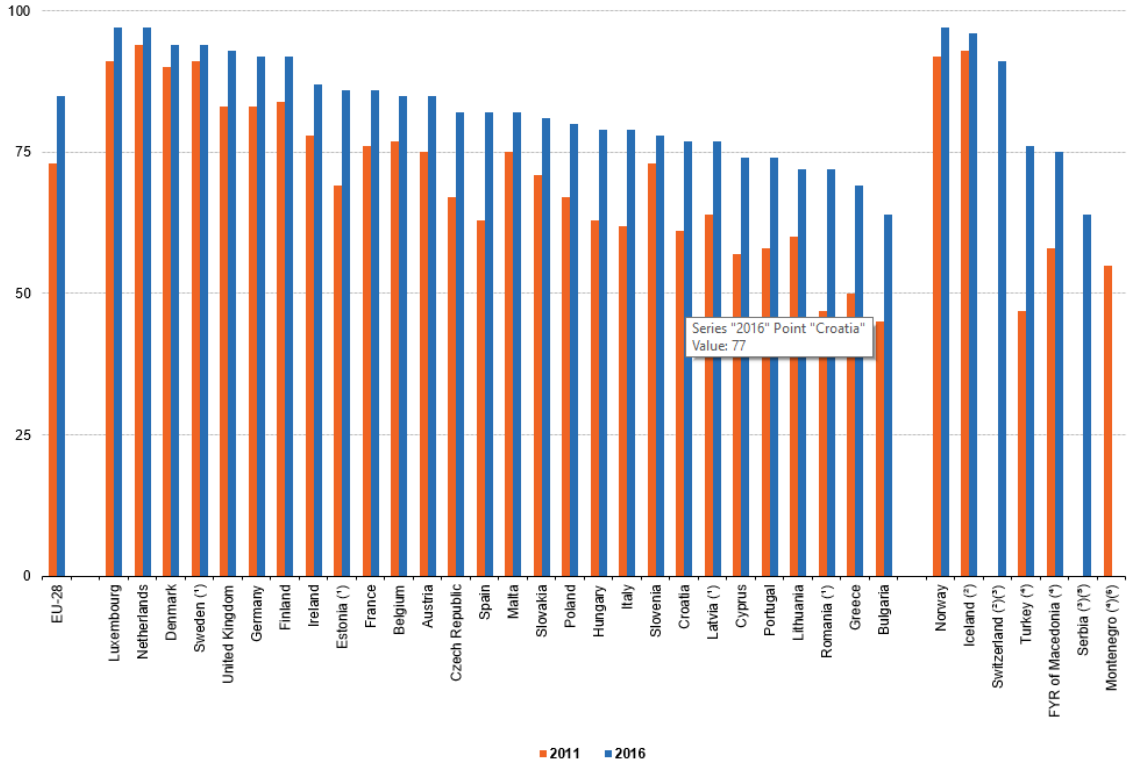
Science, technology and digital society
Digital economy and society statistics — households and individuals

Figure 1: Internet access and broadband internet connections of households, EU-28, 2007–2016
(% of all households)

	Internet access	Broadband connections
2007	55	42
2008	60	48
2009	66	56
2010	70	61
2011	73	67
2012	76	72
2013	79	76
2014	81	78
2015	83	80
2016	85	83

Source: Eurostat (online data codes: isoc_ci_in_h and isoc_ci_it_h)

Zašto GDPR?



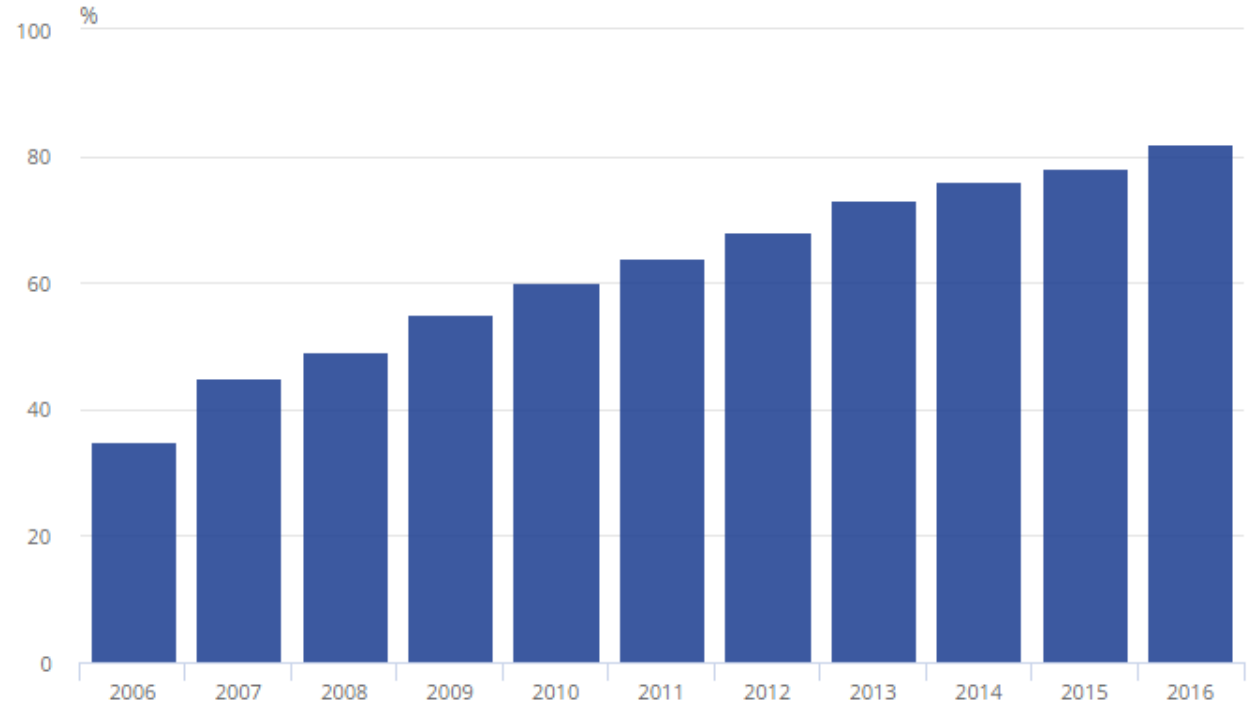
Science, technology and digital society
Digital economy and society statistics — households and individuals

Figure 2: Internet access of households, 2011 and 2016
(% of all households)

	2011	2016
EU-28	73	85

Zašto GDPR?

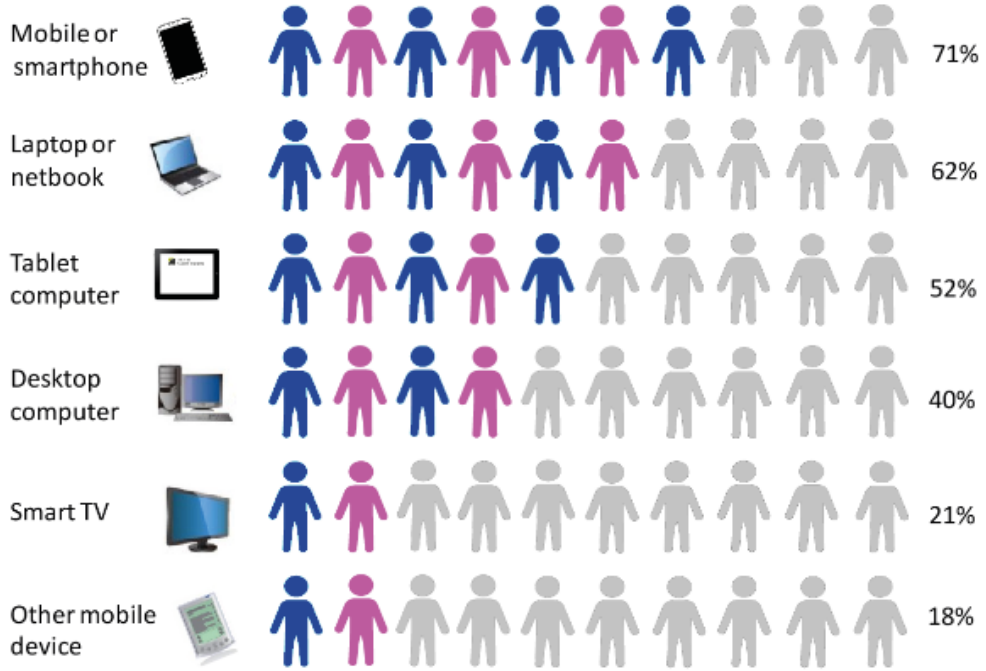
Figure 1: Daily internet use by adults, 2006 to 2016, Great Britain



Source: Office for National Statistics

Zašto GDPR?

Figure 2: Devices used to access the internet, 2016, Great Britain



Source: Office for National Statistics

2020 This Is What Happens In An Internet Minute

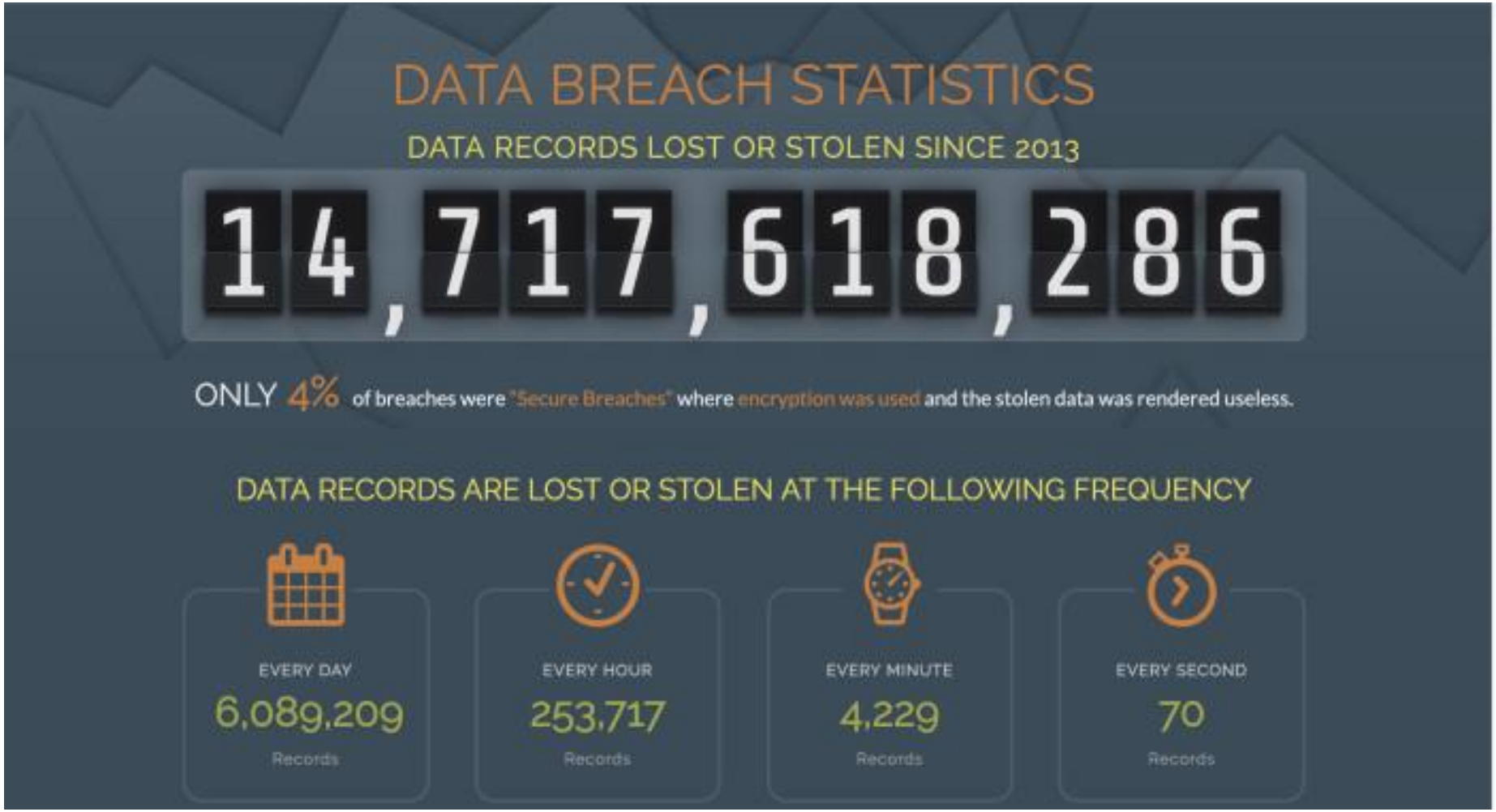
2021 This Is What Happens In An Internet Minute

ZAŠTO GDPR?

- 17.05.2017.

ZAŠTO GDPR?

- 18.06.2018.



ZAŠTO GDPR?

- 17.9.2019.

ŠTO JE TO GDPR?

- Potpuna revizija regulacije zaštite podataka s opsežnim ažuriranjima onoga što se može smatrati identificirajućim informacijama **EU građana i njihovih osobnih podataka**
- Primjena u svim državama članicama EU
- Na sve organizacije koje obrađuju podatke u EU – bez obzira na to gdje je ta organizacija geografski utemeljena
- Specifična i značajna prava za pojedince vlasnike osobnih podataka da traže naknadu, pravo na brisanje i točnu reprezentaciju

Što je to GDPR?

- Uvođenje novčanih kazni u iznosu do max. 20 mil eura ili 4% godišnjeg prometa
- Naknada se može tražiti od organizacija i pojedinaca zaposlenih kod njih
- Značajno smanjenje tog iznosa temeljeno na provođenju tehničkih ili organizacijskih kontrola.

Što od nas traži GDPR

GDPR traži: odgovorno postupanje s osobnim informacijama, u svom najširem smislu

Obveza prema GDPR-u zahtijeva

- **Razumijevanje** podataka, da bi ih
- **Zaštitili** i
- **Upravljali** njima
- Gdje god se nalazili (baze podataka, datoteke, e-mail sustavi, storage)
- U bilo kojem formatu (strukturirani, nestrukturirani, audio, itd)

Osobni podatak

- Objektivne i subjektivne informacije (činjenice i mišljenja)
- Točne i netočne informacije
- Informacije osobne i profesionalne naravi
- Obične i osjetljive/intimne informacije
- Informacije u bilo kojem obliku, odnosno formatu / zapisu

Osobni podatak

Osobni podatak	Posebne kategorije osobnih podataka	Podaci koji se odnose na kaznene osude i kažnjiva djela
Sve informacije	rasno ili etničko podrijetlo, politička mišljenja, vjerska ili filozofska uvjerenja ili članstvo u sindikatu; genetski podaci, biometrijski podaci, podaci koji se odnose na zdravlje ili spolni život ili seksualnu orijentaciju (članak 9.)	Podaci koji se odnose na kaznene osude i kažnjiva djela ili povezane mjere sigurnosti (članak 10.)

Osobni podatak

informacija	koja se „odnosi”	na „pojedinca”	čiji identitet je utvrđen ili se može utvrditi

Kad se informacija odnosi na pojedinca?

1. Kada je informacija „o pojedincu” (relevantan je sadržaj)
2. Kada se informacija obrađuje s ciljem da se na bilo koji način utječe na status ili ponašanje pojedinca (relevantan je razlog obrade)
3. Kad obrada informacije može imati utjecaj na prava i interese ispitanika (relevantan je rezultat obrade).

Osobni podatak

- Pojedinac = fizička osoba
- Podaci umrlih osoba? Podaci nerođene djece?
- Podaci fizičkih osoba koje obavljaju posebne funkcije (državni dužnosnici, državni i javni službenici…)?
- Pravne osobe ne uživaju zaštitu po Općoj uredbi (ali mogu po drugim pravnim izvorima)

Osobni podatak

informacija → koja se „odnosi” → na „pojedinca” → čiji identitet je utvrđen ili se može utvrditi

Identitet je utvrđen	Identitet se može utvrditi
Pero Perić, OIB: 28717983254, radi na Ekonomskom fakultetu Sveučilišta u Zagrebu kao profesor	Vozač automobila registarskih oznaka ZG-123-XY počinio je prometni prekršaj jer je vozio iznad dopuštenog ograničenja brzine

Osobni podatak

informacija | koja se „odnosi” | na „pojedinca” | čiji identitet je utvrđen ili se može utvrditi

Pojedinac čiji identitet se „može utvrditi”

1. Samo teoretska mogućnost identificiranja pojedinca nije dovoljna!!
2. Ali, nije potrebno da se identitet zaista utvrdi, nego samo da može biti utvrđen
3. Tko mora moći utvrditi identitet pojedinca?
4. Kad se identitet može utvrditi (koji standard se primjenjuje)?
5. Koje mogućnosti za potencijalno utvrđivanje identiteta su relevantne?

Propisi o zaštiti osobnih podataka ne primjenjuju se na anonimizirane informacije

Anonimne informacije (podaci)

informacije koje se ne odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi

Anonimne informacije (podaci)

Prosječna plaća u trgovačkom društvu AB je XXXXX HRK.

Primjer: čisti osobni podaci

Prezime, ime	Prijava	Broj noćenja	Broj gostiju	Smještaj	Dodatne usluge	Ukupno
Horvat, Ema	01-09-2017	7	2	7500,00	0,00	7500,00
Novak, Ana	14-3-2017	6	2	6200,00	0,00	6200,00
Marić, Luka	12-12-2017	7	1	6000,00	150,00	6150,00
Jurić, Marko	18-11-2017	8	1	7800,00	180,00	7980,00
Petrović, Mia	23-10-2017	4	3	4210,00	0,00	4210,00
Matić, Jakov	01-02-2018	6	2	8000,00	580,00	8580,00
Radić, Ivan	04-01-2018	5	3	4900,00	0,00	4900,00
Božić, Mia	10-02-2018	3	1	3750,00	0,00	3750,00
Stipić, Lucija	14-02-2018	1	2	2100,00	2000,00	4100,00

Primjer: anonimizirani podaci

Prezime, ime	Prijava	Broj noćenja	Broj gostiju	Smještaj	Dodatne usluge	Ukupno
XY	01-09-2017	7	2	7500,00	0,00	7500,00
XY	14-3-2017	6	2	6200,00	0,00	6200,00
XY	12-12-2017	7	1	6000,00	150,00	6150,00
XY	18-11-2017	8	1	7800,00	180,00	7980,00
XY	23-10-2017	4	3	4210,00	0,00	4210,00
XY	01-02-2018	6	2	8000,00	580,00	8580,00
XY	04-01-2018	5	3	4900,00	0,00	4900,00
XY	10-02-2018	3	1	3750,00	0,00	3750,00
XY	14-02-2018	1	2	2100,00	2000,00	4100,00

Pseudonimizirane informacije (podaci)

informacije koje se više ne mogu pripisati određenom ispitaniku bez uporabe ***dodatnih informacija***

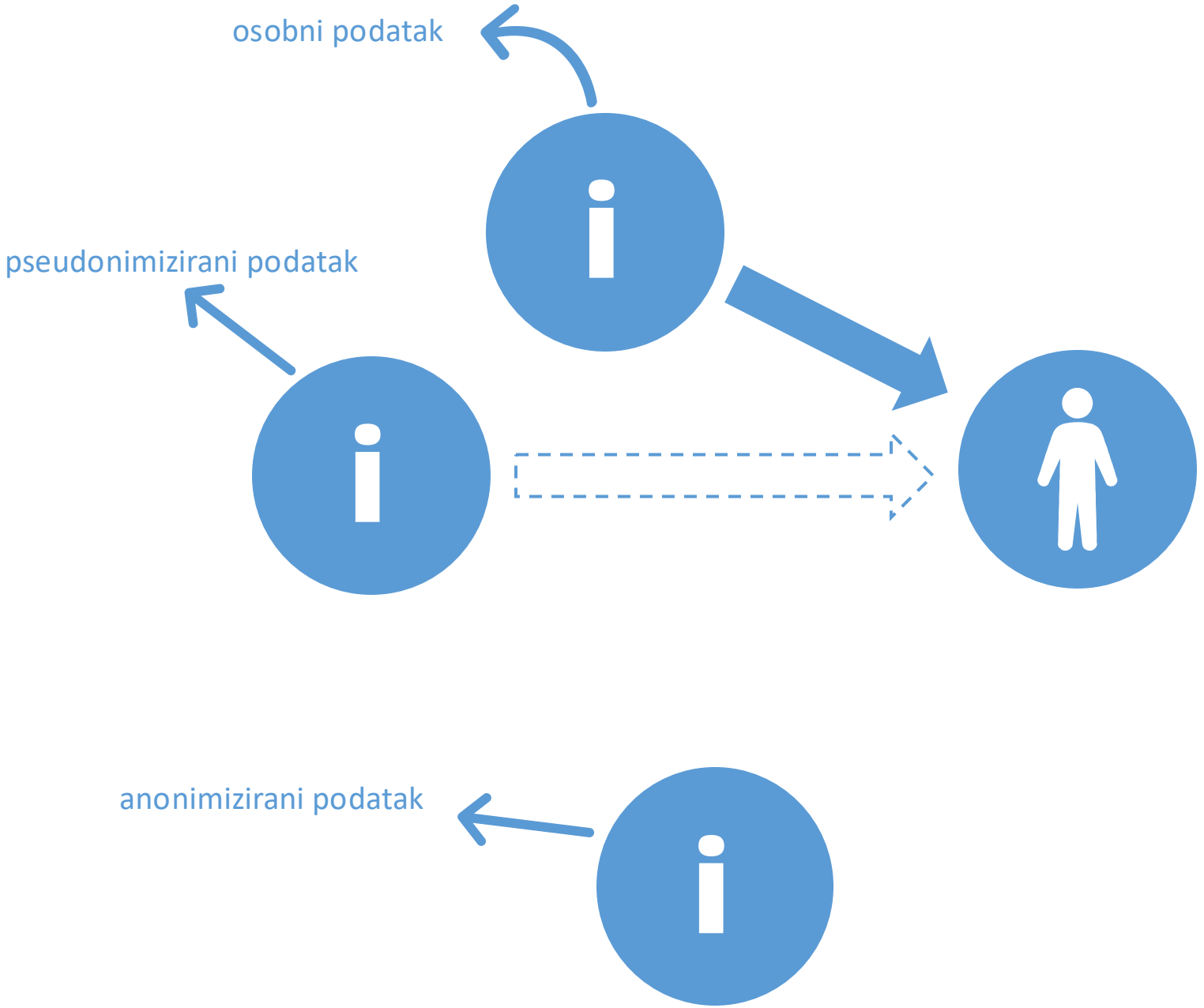
Primjer: pseudonimizirani podaci

Sustav A

Prezime, ime	Šifra
Horvat, Ema	465sdfte
Novak, Ana	4465er7t
Marić, Luka	ikgswr45
Jurić, Marko	8gksrt
Petrović, Mia	88zisrt
Matić, Jakov	azq63
Radić, Ivan	5596zew
Božić, Mia	ir94546g
Stipić, Lucija	nah645

Sustav B

Šifra	Prijava	Broj noćenja	Broj gostiju	Smještaj	Dodatne usluge	Ukupno
465sdfte	01-09-2017	7	2	7500,00	0,00	7500,00
4465er7t	14-3-2017	6	2	6200,00	0,00	6200,00
ikgswr45	12-12-2017	7	1	6000,00	150,00	6150,00
8gksrt	18-11-2017	8	1	7800,00	180,00	7980,00
88zisrt	23-10-2017	4	3	4210,00	0,00	4210,00
azq63	01-02-2018	6	2	8000,00	580,00	8580,00
5596zew	04-01-2018	5	3	4900,00	0,00	4900,00
ir94546g	10-02-2018	3	1	3750,00	0,00	3750,00
nah645	14-02-2018	1	2	2100,00	2000,00	4100,00


osobni podatak
pseudonimizirani podatak
anonimizirani podatak

Što je to „obrada osobnih podataka”?

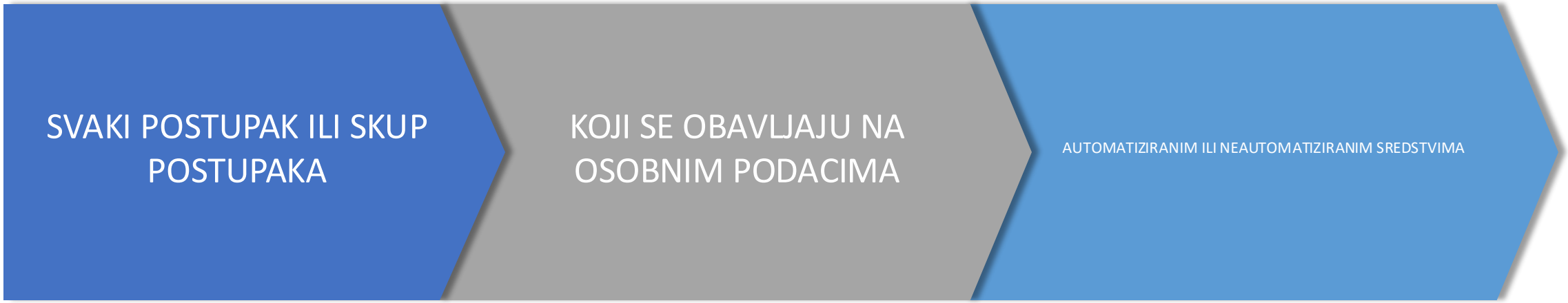
OBRADA OSOBNIH PODATAKA

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;

OBRADA OSOBNIH PODATAKA



Javna objava podataka

- Navođenje osobnih podataka fizičke osobe na mrežnim stranicama je „obrada” tih podataka

Aktivnosti internetskih pretraživača

- Radnje internetskog pretraživača (indeksiranje, privremena pohrana, pronalaženje, rangiranje) koje se poduzimaju na osobnih podacima su „obrada” koja ulazi u polje primjene propisa o zaštiti osobnih podataka

Samo privremena (prolazna) obrada podataka?

Primjenjuje li se Opća uredba na slučajeve prolazne i kratkotrajne obrade osobnih podataka? (npr. videonadzor bez snimanja)

Teritorijalno polje primjene

Teritorijalno polje primjene

Ako voditelj ili izvršitelj obrade imaju poslovni nastan u EU

Ako voditelj ili izvršitelj, koji nemaju poslovni nastan u EU, nude robu ili usluge ispitanicima u EU

Ako voditelj ili izvršitelj, koji nemaju poslovni nastan u EU, prate ponašanje ispitanika koje se odvija u EU

Svrha obrade podataka; načelo ograničenja svrhe

Koja je svrha obrade?

Svrha = cilj obrade podataka, razlog zbog kojeg se podaci obrađuju

Definiranje svrhe je kamen temeljac za primjenu drugih načela obrade podataka

Definiranje svrhe je nužni preduvjet za određivanje pravnih temelja obrade podataka

Iz perspektive ispitanika, definiranje svrhe je nužno za transparentnost, predvidljivost i mogućnost vršenja kontrole

Načelo ograničavanja svrhe (čl. 5/1/b)

OP moraju biti prikupljeni u posebne, izričite i zakonite svrhe

OP ne smiju se dalje koristiti na način koji nije u skladu s inicijalnom svrhom

„posebna” (*specified*) = određena, utvrđena

Koliko detaljno svrha mora biti određena?

Primjerice:
„podaci se obrađuju u marketinške svrhe”
„podaci se obrađuju radi slanja obavijesti o novim proizvodima i uslugama putem e-maila”

Načelo ograničavanja svrhe (čl. 5/1/b)

OP moraju biti prikupljeni u posebne, izričite i zakonite svrhe

OP ne smiju se dalje koristiti na način koji nije u skladu s inicijalnom svrhom

Ime i prezime, poštanska adresa

Svrha: slanje proizvoda i računa na kućnu adresu nakon teleprodaje

Slanje kataloga s drugim proizvodima istog prodavatelja?

Kad je obrada u sekundarnu svrhu dopuštena? (1)

- Kada se temelji na pravu Unije ili pravu države članice koje predstavlja nužnu i razmjernu mjeru u demokratskom društvu za zaštitu ciljeva iz članka 23. stavka 1:
  - (a) nacionalne sigurnosti;
  - (b) obrane;
  - (c) javne sigurnosti;
  - (d) sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenopravnih sankcija, uključujući zaštitu od prijetnji javnoj sigurnosti i njihovo sprečavanje;
  - (e) drugih važnih ciljeva od općeg javnog interesa Unije ili države članice, osobito važnog gospodarskog ili financijskog interesa Unije ili države članice, što uključuje monetarna, proračunska i porezna pitanja, javno zdravstvo i socijalnu sigurnost;
  - (f) zaštite neovisnosti pravosuđa i sudskih postupaka;
  - (g) sprečavanja, istrage, otkrivanja i progona kršenja etike za regulirane struke;
  - (h) funkcije praćenja, inspekcije ili regulatorne funkcije koja je, barem povremeno, povezana s izvršavanjem službene ovlasti u slučajevima iz točaka od (a) do (e) i točke (g);
  - (i) zaštite ispitanika ili prava i sloboda drugih;
  - (j) ostvarivanja potraživanja u građanskim sporovima

Kad je obrada u sekundarnu svrhu dopuštena? (2)

- Ako postoji privola ispitanika, ili

Kad je obrada u sekundarnu svrhu dopuštena? (3)

- Ako je sekundarna obrada *sukladna* inicijalnoj, pri čemu se uzima u obzir:
  - (a) svaku vezu između svrha prikupljanja osobnih podataka i svrha namjeravanog nastavka obrade;
  - (b) kontekst u kojem su prikupljeni osobni podaci, posebno u pogledu odnosa između ispitanikâ i voditelja obrade;
  - (c) prirodu osobnih podataka, osobito činjenicu obrađuju li se posebne kategorije osobnih podataka u skladu s člankom 9. ili osobni podaci koji se odnose na kaznene osude i kažnjiva djela u skladu s člankom 10.;
  - (d) moguće posljedice namjeravanog nastavka obrade za ispitanike;
  - (e) postojanje odgovarajućih zaštitnih mjera, koje mogu uključivati enkripciju ili pseudonimizaciju.

Načelo smanjenja količine podataka

Načelo „smanjenja količine podataka” – čl. 5/1/c

- Osobni podaci moraju biti primjereni, relevantni i ograničeni na ono što je nužno u odnosu na svrhe u koje se obrađuju („smanjenje količine podataka”)

Podaci su prikladni za ostvarivanje svrhe

Svrha se ne bi razumno mogla postići bez obrade te količine podataka

Prekomjerna obrada podataka

Nadalje, u čl. 93. st. 4. Zakona o vlasništvu i drugim stvarnim pravima je izrijekom propisano da je upravitelj dužan, između ostalog, položiti svakom suvlasniku uredan račun o poslovanju u prethodnoj kalendarskoj godini i staviti mu na prikladan način na uvid isprave na kojima se temelji, i to najkasnije do 30. lipnja svake godine.

Slijedom navedenog, može se razabrati jasna dužnost upravitelja prema svakom od suvlasnika nekretnine, međutim da bi isti ispunio navedenu obvezu koja proizlazi iz Zakona n**ije nužno da pojedinom suvlasniku otkriva/dostavlja primjerice, kako navodite, IBAN njegovih susjeda ili bilo kojeg drugog uplatitelja (uz ime i prezime/naziv uplatitelja/pravne ili fizičke osobe kojoj je izvršena isplata, datum i mjesto uplate/isplate te iznos uplate/isplate),** a za koji se u načelu može razabrati da nije nužan za pružanje informacija o stanju zajedničkog računa odnosno poslovanju u prethodnoj godini.

AZOP, mišljenje od 15. 2. 2022.

Oznaka operatera na računu

Slijedom navedenog, a sukladno Zakonu o porezu na dodanu vrijednost i Zakonu o fiskalizaciji u prometu gotovinom razvidno je kako su navedenim propisima predviđeni obvezni elementi koje račun mora sadržavati, te je kao jedan od obvezatnih elemenata računa i oznaka operatera. Dakle, s aspekta zaštite osobnih podataka, ova Agencija drži da bi račun koji ispostavlja pravna osoba u dijelu u kojem je navedena „oznaka operatera", u konkretnom slučaju ime i prezime zaposlenika koji obavlja poslove naplate na naplatnom uređaju, predstavljao prekomjernu obradu osobnih podataka te za isti ne nalazimo pravnu osnovu u citiranim Zakonima. Primjenom načela razmjernosti i smanjene količine podataka u postupku obrade osobnih podataka poslodavac je dužan voditi brigu o opsegu osobnih podataka koji se obrađuje na način da se u svrhu zaštite privatnosti zaposlenika istakne eventualno ime zaposlenika ili nekazujuća šifra.

AZOP, mišljenje od 5. 6. 2019.

Pravni temelji za obradu podataka („zakonitost obrade”)

Pravni temelji za obradu podataka

- Predstavljaju polaznu točku za ocjenu zakonitosti obrade podataka
- Čl. 6. daje odgovor na pitanje smiju li se osobni podaci obrađivati, ne kako se smiju obrađivati
- Moguće je da su istodobno primjenjiva dva ili više pravnih temelja

Dopustivost miješanja u temeljno ljudsko pravo

Tri skupine pravila o zakonitosti obrade

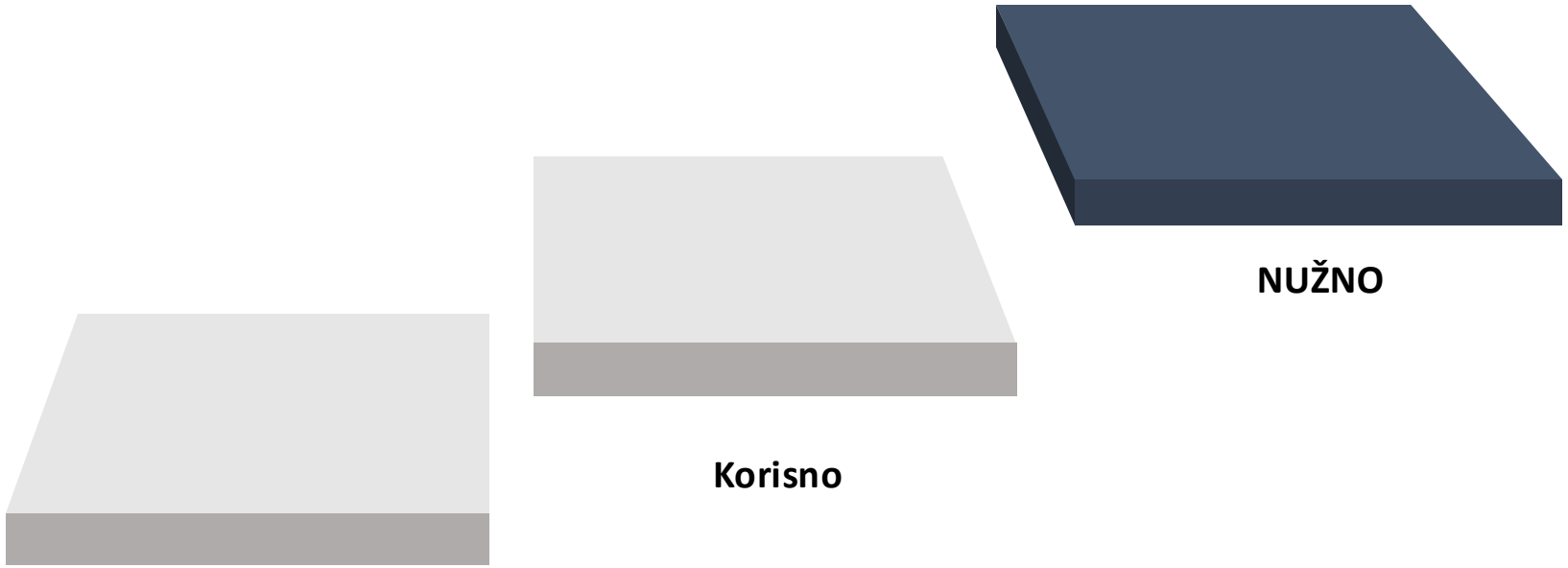
PRAVNI TEMELJ ZA OBRADU PODATAKA („zakonitost obrade”)

- Privola ispitanika
- Pravni temelji određeni propisima

Pravni temelji za obradu osobnih podataka („zakonitost obrade”, čl. 6.)

T.	Pravni temelj	Posebni zahtjev nužnosti
(a)	Privola ispitanika	NE
(b)	Sklapanje i izvršavanje ugovora	DA
(c)	Poštivanje pravnih obveza voditelja obrade	DA
(d)	Zaštita ključnih interesa ispitanika ili druge fizičke osobe	DA
(e)	Izvršavanje zadaće od javnog interesa ili izvršavanje službene ovlasti voditelja obrade	DA
(f)	Legitimni interes voditelja obrade ili treće strane	DA

Što znači „nužno” u kontekstu čl. 6/1/b-f?



Što znači „nužno” u kontekstu čl. 6/1/b-f? Stroga nužnost ili balansiranje?

Osobni podaci trebali bi se obrađivati samo ako se svrha obrade razumno (*reasonably*) ne bi mogla postići drugim sredstvima.

Uredba, recital 39.

Pravni temelji određuju se u odnosu na deklariranu svrhu obrade podataka

Privola ispitanika

⚠ OBRADA OSOBNIH PODATAKA

Odabirom opcije „U redu“ dajem svoju izričitu suglasnost i privolu da Ministarstvo financija, Porezna uprava (u daljnjem tekstu Porezna uprava) prikuplja, obrađuje, koristi i analizira podatke koji se odnose na mene, uključujući i moje osobne podatke. Privola se izričito odnosi na podatke koje sam dala/dao Poreznoj upravi prilikom registracije na elektroničke usluge porezne uprave (ePorezna).

Ovime dajem izričitu privolu Poreznoj upravi da može poduzimati radnje vezano za obradu mojih osobnih podataka u skladu s propisima koji uređuju zaštitu osobnih podataka, a u svrhu obavljanja osnovnih djelatnosti Porezne uprave koji proizlaze iz Općeg poreznog zakona (NN 115/16) i Zakona o Poreznoj uprava (NN 115/16).

Odabirom opcije „U redu“, potvrđujem da sam prije davanja suglasnosti obaviještena/obaviješten o sljedećem:

- suglasnost dajem dobrovoljno
- da sam informiran o svrsi obrade kojoj su podaci namijenjeni
- suglasnost mogu opozvati te Porezna uprava nakon toga više neće obrađivati podatke u svrhu za koju je suglasnost bila dana, osim podataka koji su nužni za izvršavanje zadaća od javnog interesa odnosno koji se temelje na službenoj ovlasti Porezne uprave
- opoziv suglasnosti ne utječe na zakonitost obrade prije njezina opoziva
- Porezna uprava će čuvati podatke o suglasnosti i obradama kako bi dokazala zakonitost obrade

Ova privola vrijedi do opoziva.

„Ovime dajem izričitu privolu Poreznoj upravi da može poduzimati radnje vezano za obradu mojih osobnih podataka u skladu s propisima koji uređuju zaštitu osobnih podataka, a u svrhu obavljanja osnovnih djelatnosti Porezne uprave koji proizlaze iz Općeg poreznog zakona (NN 115/16) i Zakona o Poreznoj uprava (NN 115/16).”

Privola ispitanika

Kako se daje?	Kakva mora biti?	Na što se odnosi?
izjavom, ili	dobrovoljna	Obradu osobnih podataka u određenu svrhu
jasnom potvrdnom radnjom	specifična	
	informirana	
	nedvosmislena	

Forma privole

- Uredba ne postavlja zahtjeve u pogledu forme privole. Mogla bi se dati i usmenom izjavom.
- Međutim, *teret dokaza o postojanju privole je na voditelju obrade*
- U praksi, neophodno će biti osigurati dokaz o danoj privoli
- Privola mora biti predočena na jasan način, u razumljivom i lako dostupnom obliku, uporabom jasnog i jednostavnog jezika, inače *nije pravno obvezujuća*
- Ispitanik ima pravo povući privolu; povlačenje mora biti jednako jednostavno kao i davanje
- Posebna pravila za privolu od strane djeteta ili u slučajevima obrade posebnih kategorija osobnih podataka

Nužnost u kontekstu ugovornog odnosa

Obrada podataka je nužna

Za izvršavanje ugovora u kojem je ispitanik stranka

Za poduzimanje radnji na zahtjev ispitanika prije sklapanja ugovora

Obrada podataka nužna za izvršavanje ugovora u kojemu je ispitanik stranka

- Ugovor može biti između ispitanika i
  - Voditelja obrade
  - Treće osobe

- Koji podaci se mogu prikupljati po ovom pravnom temelju?
  - Relevantan je sadržaj i cilj ugovora
  - Podaci moraju biti *bona fide* nužni za izvršavanje ugovora

Može li čl. 6/1/b („obrada nužna za izvršavanje ugovora u kojemu je ispitanik stranka”) biti pravni temelj za obradu podataka u svrhu slanja opomena i obavijest (pred tužbu, ovrhu, …)?

Može li ista norma biti temelj za prijenos podataka agenciji za naplatu (nakon cesije potraživanja) u odnosu na one ispitanike koji nisu podmirili svoje obveze iz ugovora?

Obrada podataka nužna za poduzimanje radnih za zahtjev ispitanika u predugovornoj fazi

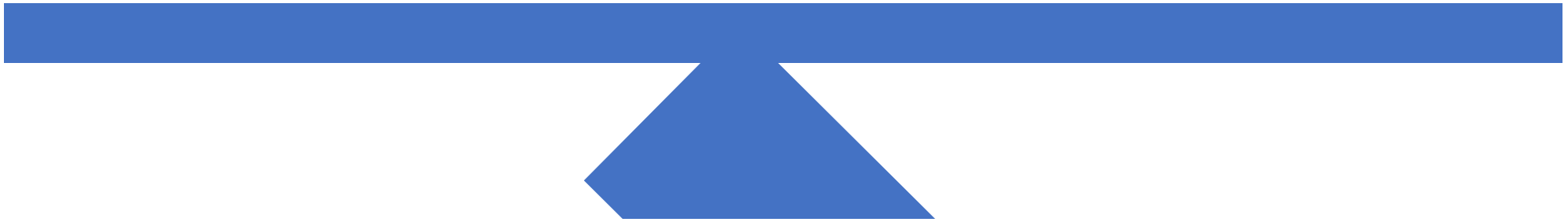
- Primjerice:
  - Ispitanik zatraži informativnu ponudu
  - Ispitanik popuni zahtjev za sklapanje ugovora

- Ključno je da inicijativa dolazi od ispitanika, a ne od voditelja obrade

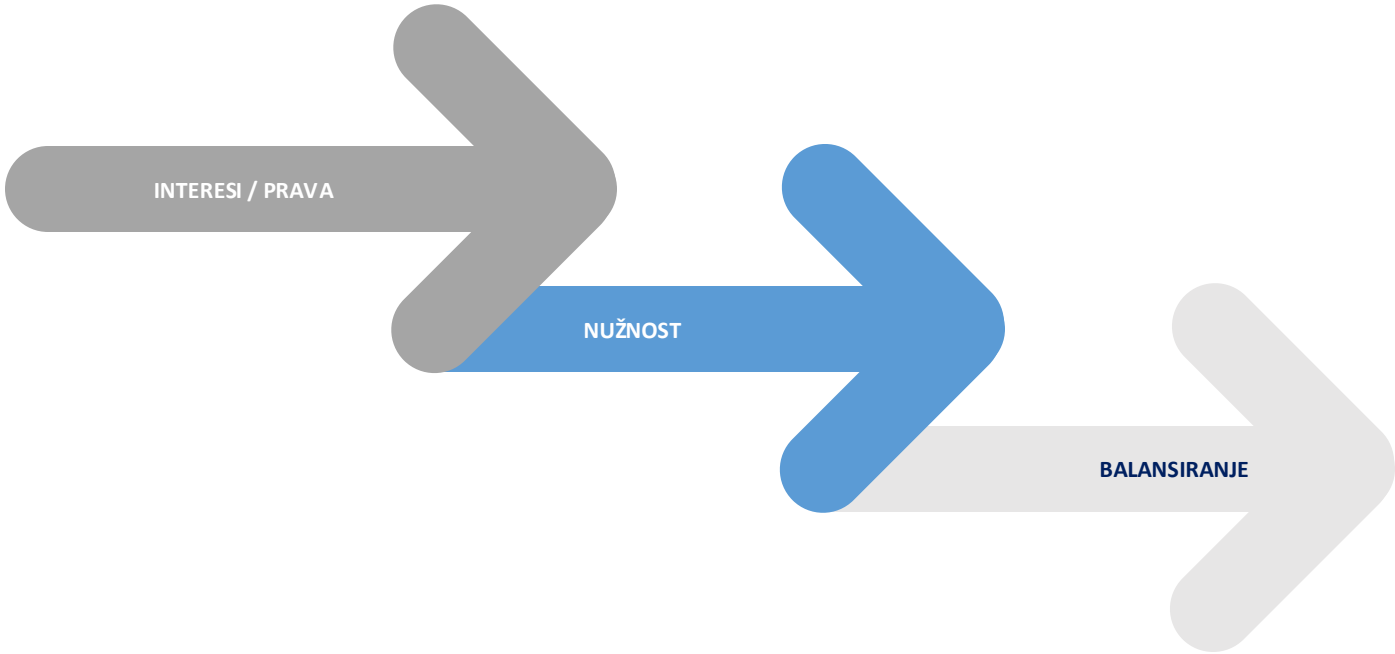
Legitimni interes voditelja obrade ili treće strane

Voditelj obrade /
treća strana

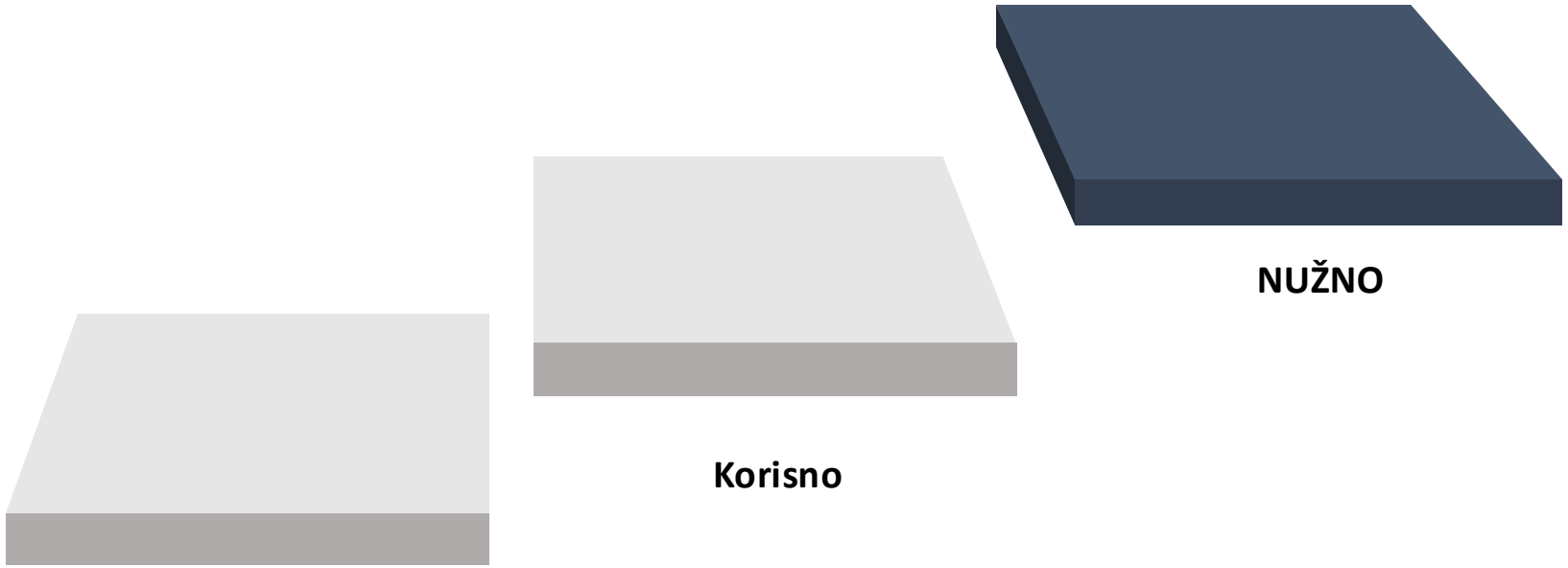
Ispitanik



„obrada je nužna za potrebe legitimnih interesa voditelja obrade ili treće strane, osim kada su od tih interesa jači interesi ili temeljna prava i slobode ispitanika koji zahtijevaju zaštitu osobnih podataka, osobito ako je ispitanik dijete”.


INTERESI / PRAVA
NUŽNOST
BALANSIRANJE

Nužnost



Interesi / prava

Interes(i) voditelja obrade

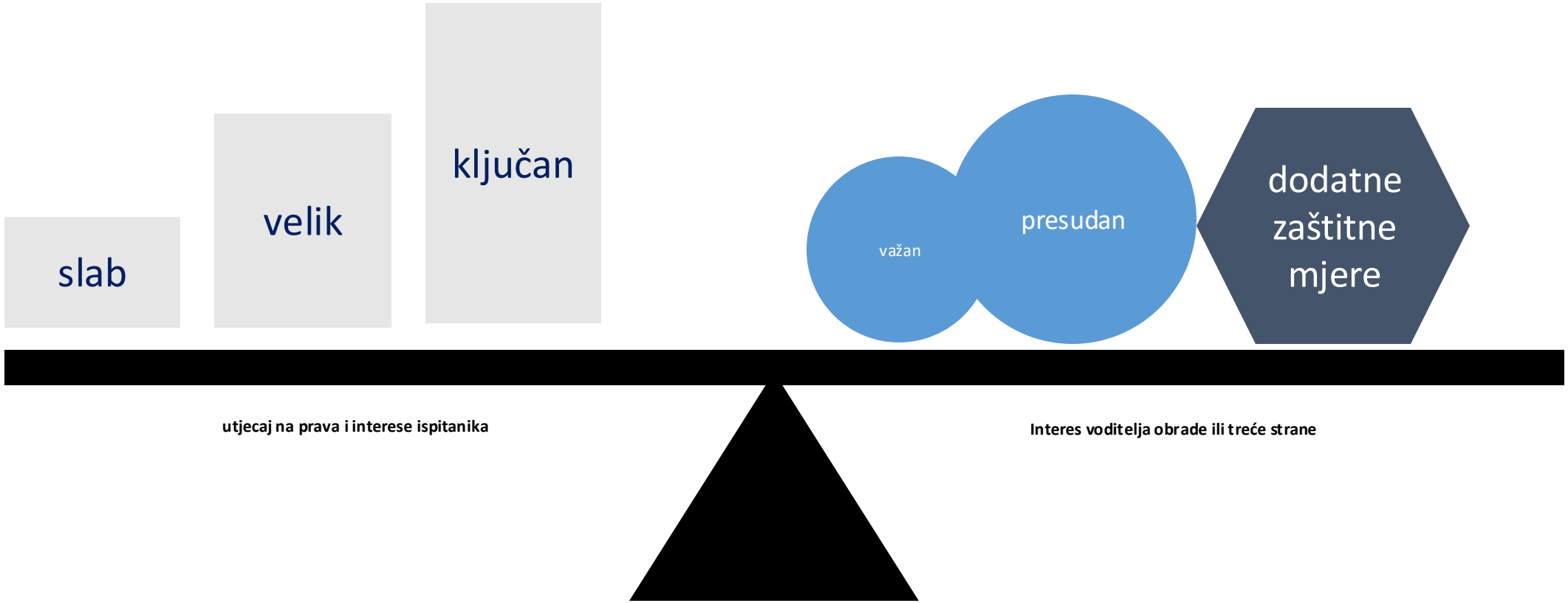
- Širi pojam od svrhe obrade podataka
- Širok raspon mogućih interesa
- Mora biti stvaran i prisutan u konkretnom slučaju
- Mora biti legitiman; legitiman je ako je u skladu s pravom

- Primjeri: poslovni odnos, sprječavanje prijevara, izravni marketing, mrežna i informacijska sigurnost, prijenos unutar grupe za Internet potrebe, ispunjenje tražbina, sprječavanje pranja novca, ….

Interesi / prava ispitanika

- Široko definirani
- Ne moraju biti „legitimni”
- Posebna važnost ako je ispitanik dijete

Balansiranje interesa i prava



Legitimni interes i načelo transparentnosti

- Obrada podataka temeljem legitimnog interesa ne obavlja se u tajnosti
- Voditelj obrade mora napraviti test iz čl. 6/1/f i dokumentirati ga
- Pravila o transparentnosti (čl. 13. i 14.) primjenjuju se (voditelj obrade dužan je informirati ispitanika)
- Ispitanik ima pravo na prigovor (čl. 21.), u kojem slučaju voditelj obrade mora dokazati da je zadovoljen test iz čl. 6/1/f.

Obrada je nužna radi poštovanja pravnih obveza voditelja obrade (točka c) ili za izvršavanje zadaće od javnog interesa ili pri izvršavanju službene ovlasti voditelja obrade (točka e)

- Pravne obveze utvrđuju se u nacionalnom pravu ili pravu EU. Ne mora biti riječ o zakonima (aktima parlamenta)
- U njemačkoj doktrini, smatra se da pravna obveza može nastati i temeljem kolektivnog ugovora

Primjeri

- Obrada osobnih podataka za potrebe državnih tijela
- Obrada osobnih podataka za potrebe medija
- Pristup informacijama u posjedu tijela javne vlasti

Primjer: obrada nije nužna

- Objava na mrežnim stranicama doma zdravlja u okviru godišnjeg izvješća podataka o sporu s podnositeljicom zahtjeva nije nužna jer nije predviđena zakonom

AZOP, rješenje od 28. kolovoza 2019.

Primjer: odnos Opće uredbe i posebnog propisa

Slijedom navedenog, u ovoj upravnoj stvari utvrđeno je da su na web stranici objavljeni podaci koji se, između ostaloga, odnose na Zdravstvenu ustanovu, Specijalnu bolnicu za medicinsku rehabilitaciju kao tijela javne vlasti, točnije objavljeni su dokumenti koji sadrže osobne podatke koji se odnose na podnositeljicu zahtjeva. Naime, uvidom u sadržaj predmetne stranice utvrđeno je da ista između ostaloga sadrži dokumente koji se odnose na bruto plaću, putne troškove i školovanje tj. osobne podatke podnositeljice zahtjeva. Nadalje, iz sadržaja predmetne stranice i dokumenta koji su objavljeni razvidno je da su isti dobiveni u svrhu poštivanja pravnih obveza tj. Zakona o pravu na pristup informacijama koji propisuje da su informacije dostupne svakoj domaćoj ili stranoj fizičkoj i pravnoj osobi u skladu s uvjetima i ograničenjima reguliranim u predmetnom članku. U opisanom slučaju utvrđeno je da su informacije točnije dokumenti koji sadrže osobne podatke dobiveni temeljem čl.18. Zakona o pravu na pristup informacijama te da su poštivane sve odredbe navedenog posebnog zakona posebice one koje se odnose na ograničenja odnosno zaštitu osobnih podataka iz čl.15. Zakona o pravu na pristup informacijama.

AZOP, rješenje od 15. listopada 2018.

Primjer: Mediji; „poslovni podaci”

Stoga, ova Agencija na temelju utvrđenog činjeničnog stanja u ovoj upravnoj stvari je stajališta da objavu osobnih podatka podnositeljice zahtjeva treba promatrati sa gledišta uloge i funkcije koju obavlja u društvu u kojem je zaposlena, odnosno da su osobni podaci objavljeni u sklopu profesionalne djelatnosti i posla koji ista obavlja. Naime, **osobni podaci podnositeljice spominju se u konkretnom članku u poslovnom smislu te su u tom smislu i objavljeni. Podnositeljica zahtjeva mora biti svjesna da za objavu njezinih osobnih podataka u sklopu odgovora na upit novinara, a isti je objavljen u sklopu članka u časopisu x, nije bila potrebna njezina privola za objavu njezinih osobnih podataka jer privola nije jedina pravna osnova za obradu osobnih podataka.** Objavom osobnih podataka podnositeljice u konkretnom slučaju nije došlo do povrede privatnost podnositeljice zahtjeva na radnom mjestu na način kako to regulira Opća uredba o zaštiti podataka i poseban zakon- Zakon o medijima koji izričito propisuje da nema povrede prava na zaštitu osobnih podataka ako prevladava opravdani javni interes na zaštitom privatnosti u odnosu na djelatnost novinara ili na informaciju. U konkretnom članku objavljeni su osobni podaci podnositeljice vezani uz njezine funkcije koje obavlja u društvu u kojem je zaposlena.

AZOP, rješenje od 29. travnja 2020.

Obrada je nužna radi zaštite ključnih interesa ispitanika ili druge fizičke osobe

Posebne kategorije osobnih podataka

Posebne kategorije osobnih podataka

I. rasno ili etničko podrijetlo
II. politička mišljenja
III. vjerska ili filozofska uvjerenja
IV. članstvo u sindikatu
V. genetski podaci
VI. biometrijski podaci kada se obrađuju u svrhu jedinstvene identifikacije pojedinca
VII. podaci koji se odnose na zdravlje
VIII. podaci o spolnom životu ili seksualnoj orijentaciji pojedinca

Temeljna načela

Načela obrade osobnih podataka

Zakonitost, poštenje i **transparentnost** obrade

Ograničenje svrhe

Smanjenje količine podataka

Točnost i ažurnost

Vremensko ograničenje obrade

Cjelovitosti i povjerljivosti

Odgovornost voditelja obrade za usklađenost s načelima obrade („pouzdanost”)

Koja je uloga načela iz čl. 5. Uredbe?

I. Predstavljaju izravno primjenjive odredbe koje utječu na način obrade podataka
II. Koriste se kao sredstvo za tumačenje drugih odredbi Uredbe
III. Dovodi li njihovo kršenje do sankcioniranja?

Zakonitost, poštenje i transparentnost obrade

Zakonitost

Postojanje pravne norme	Kvaliteta pravne norme
Zakon, podzakonski propis, …	Dostupnost
	Jasnoća, određenost i predvidljivost
	Zaštita od arbitrarne primjene

Zakonitost, poštenje i transparentnost obrade

Zakonitost

- Postojanje adekvatnog pravnog temelja iz čl. 6. (+ čl.. 9. ako je primjenjivo)
- Postupanje sukladno drugim odredbama Uredbe
- Postupanje sukladno posebnim propisima
  - Zakoni
  - Podzakonski propisi
  - Pravni akti EU

Zakonitost, poštenje i transparentnost obrade

Poštenje?

- Opcija A: postupanje sukladno pravilima o transparentnosti
- Opcija B: dodatno samostalno značenje. Ako da, koje?

Zakonitost, poštenje i transparentnost obrade

Transparentnost

Voditelj obrade poduzima odgovarajuće mjere kako bi se ispitaniku pružile sve informacije iz članaka 13. i 14. i sve komunikacije iz članaka od 15. do 22. i članka 34. u vezi s obradom u **sažetom**, **transparentnom**, **razumljivom** i **lako dostupnom obliku**, uz uporabu **jasnog i jednostavnog jezika**, osobito za svaku informaciju koja je posebno namijenjena djetetu.

Informacije se pružaju u **pisanom obliku ili drugim sredstvima**, među ostalim, ako je prikladno, elektroničkim putem.

Ako to zatraži ispitanik, informacije se mogu pružiti **usmenim** putem, pod uvjetom da je drugim sredstvima utvrđen identitet ispitanika.

Zakonitost, poštenje i transparentnost obrade

Je li za zakonitost obrade podataka relevantan izvor podataka?

Smije li trgovačko društvo u RH kupiti određene informacije, koje uključuju i osobne podatke građana (ime i prezime / broj telefona; ime i prezime / e-mail) od drugog trgovačkog društva i koristiti te podatke za vlastite (marketinške) aktivnosti?

Zakonitost, poštenje i transparentnost obrade

- Zakonitost
  - Postojanje adekvatnog pravnog temelja iz čl. 6. (+ čl.. 9. ako je primjenjivo)
  - Postupanje sukladno drugim odredbama Uredbe
  - Postupanje sukladno posebnim propisima
    - Zakoni
    - Podzakonski propisi
    - Pravni akti EU

- Poštenje

- Transparentnost
  - Odražava se kroz posebna pravila iz čl. 13. i 14.

Točnost podataka

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 („točnost”);

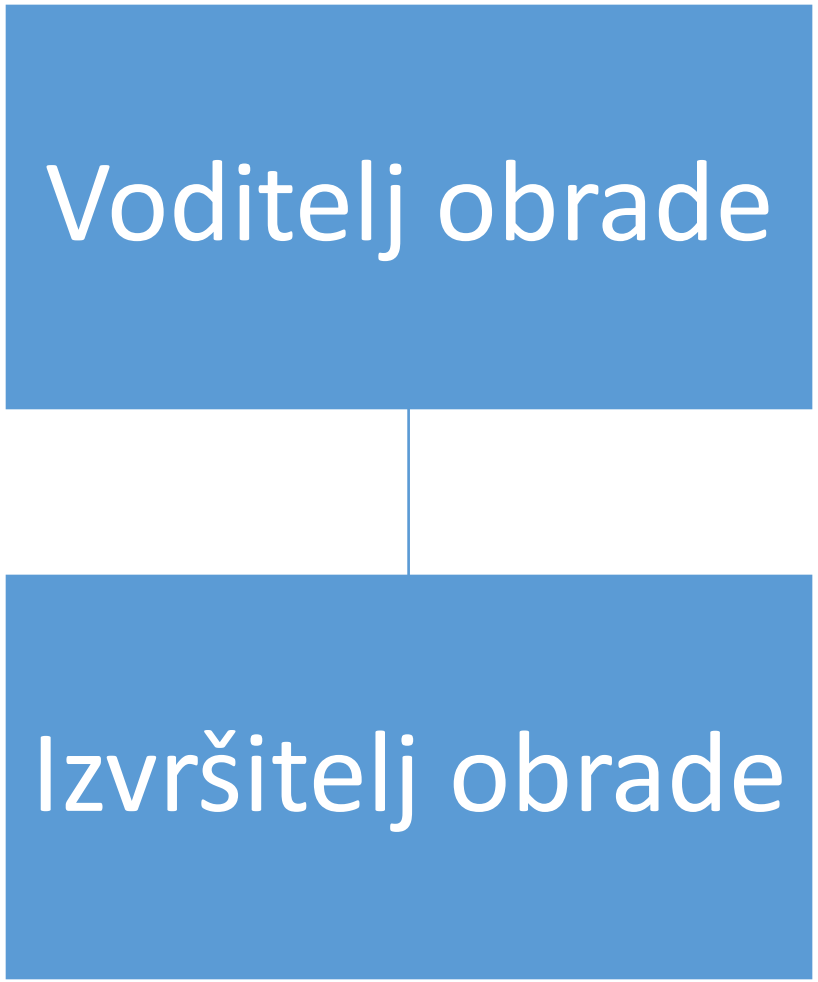
Vremensko ograničenje pohrane

- Osobni podaci moraju biti čuvani u obliku koji omogućuje identifikaciju ispitanikâ samo onoliko dugo koliko je potrebno u svrhe radi kojih se osobni podaci obrađuju; osobni podaci mogu se pohraniti na dulja razdoblja ako će se osobni podaci obrađivati isključivo u svrhe arhiviranja u javnom interesu, u svrhe znanstvenog ili povijesnog istraživanja ili u statističke svrhe u skladu s člankom 89. stavkom 1., što podliježe provedbi primjerenih tehničkih i organizacijskih mjera propisanih ovom Uredbom radi zaštite prava i sloboda ispitanika („ograničenje pohrane”);

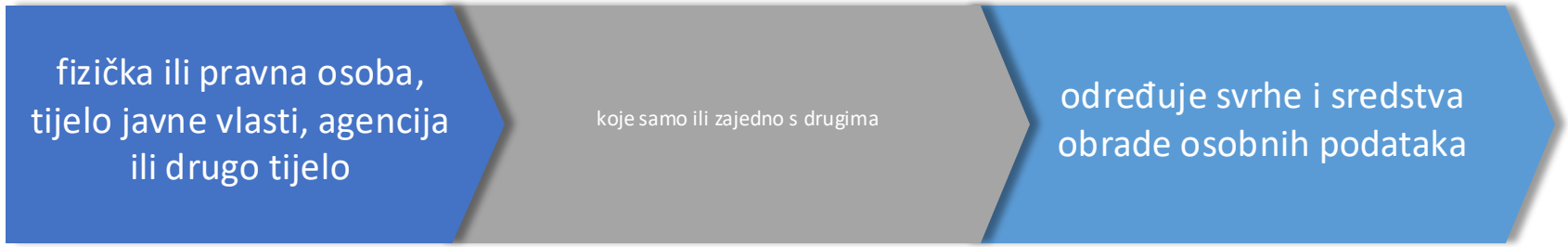
- Politika pohrane podataka
  - Koji podaci se čuvaju, u kojem obliku, na kojem mjestu
  - Koji je period pohrane za pojedinu kategoriju podataka
  - U kojim rokovima se podaci brišu
  - Tko je odgovoran za brisanje
  - Na koji način se provodi brisanje (ručno / automatski)

Odgovorni subjekti

Odgovorni subjekti



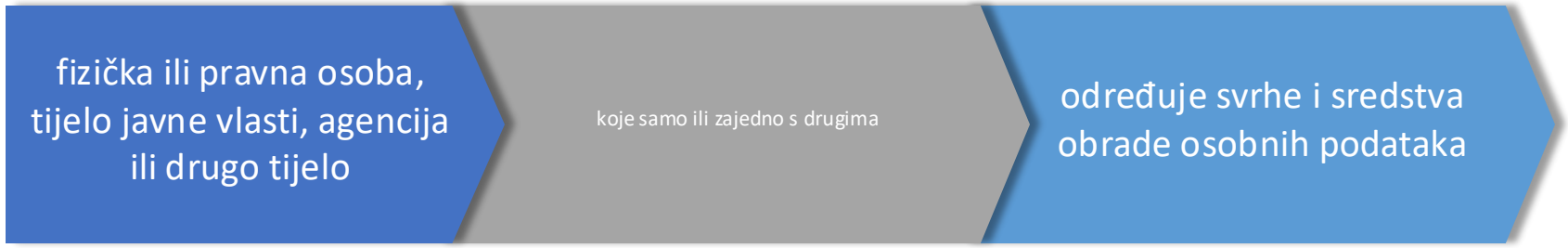
Voditelj obrade osobnih podataka



Kad je fizička osoba voditelj obrade podataka?

Je li fizička osoba unutar pravne osobe voditelj obrade?

Voditelj obrade osobnih podataka



ZAŠTO se podaci obrađuju?

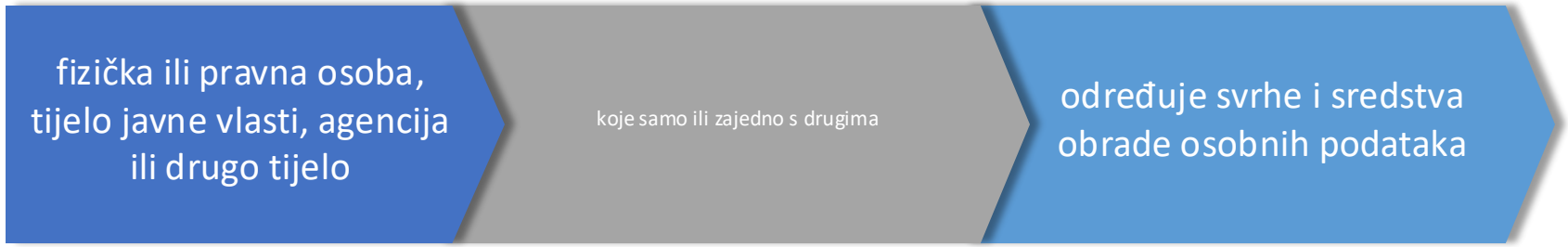
Određuje **svrhu** obrade podataka (ili više njih)

KAKO se podaci obrađuju?

Određuje bitna **sredstva** obrade osobnih podataka

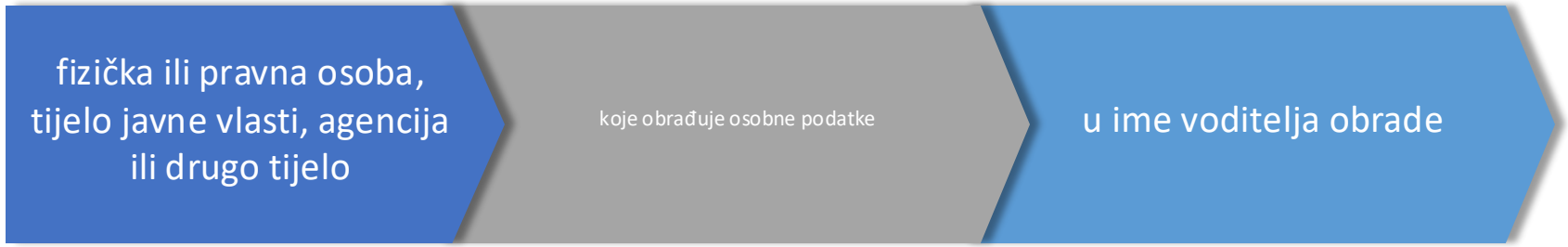
Koji podaci, na koji rok, kad se brišu, tko im ima pristup, …

Kako razlikovati samostalnog od zajedničkih voditelja obrade?



Ako dvoje ili više voditelja obrade zajednički odrede svrhe i načine obrade, oni su zajednički voditelji obrade

Izvršitelj obrade osobnih podataka



Postupa po nalogu voditelja obrade

Ako prekorači granice naloga postaje voditelj

Kako razlikujemo voditelja i izvršitelja obrade?

	Voditelj obrade	Izvršitelj obrade
Samostalno određuje svrhe obrade	DA	NE
Postupa po tuđim uputama	NE	DA
Određuje koji podaci se obrađuju, koliko dugo će biti pohranjeni, kad se moraju brisati, tko ih može koristiti (bitna pitanja načina obrade)	DA	NE
Određuje tehnička i organizacijska pitanja (sekundarna pitanja načina obrade)	U pravilu NE	U pravilu DA
Koristi podatke u vlastite svrhe	DA	NE
Unosi podatke u vlastite baze podataka	DA	NE
Nalazi se u izravnom pravnom odnosu s ispitanikom	DA	NE

Što uzimamo u obzir pri razlučivanju uloga individualnog voditelja, zajedničkih voditelja i izvršitelja obrade

I. Faktične odnose, podjele nadležnosti i uloge
II. Ugovorne odnose i nadležnosti

Prava ispitanika

Prava ispitanika

Pravo na transparentnost (pravo biti obaviješten o obradi podataka)

Pravo na pristup

Pravo na ispravak

Pravo na brisanje

Pravo na ograničenje obrade

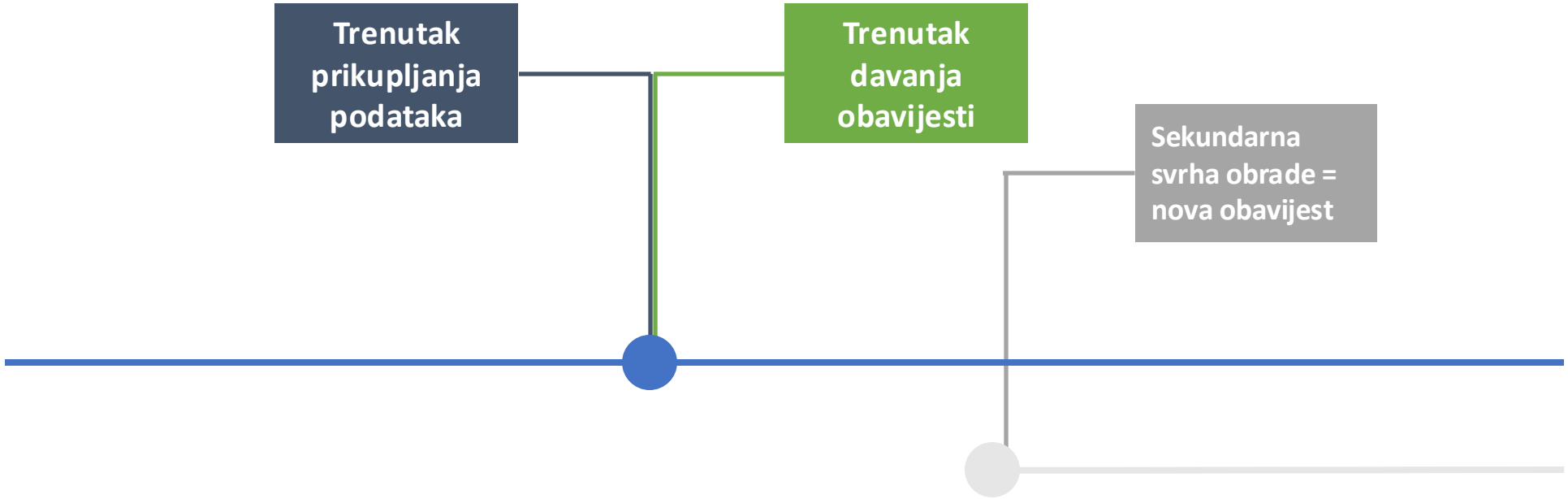
Pravo na prenosivost podataka

Pravo na prigovor

Automatizirano donošenje odluka i profiliranje

Pravo na transparentnost obrade podataka (pravo biti obavješten o obradi podataka)

Ako su podaci dobiveni od ispitanika (čl. 13.)

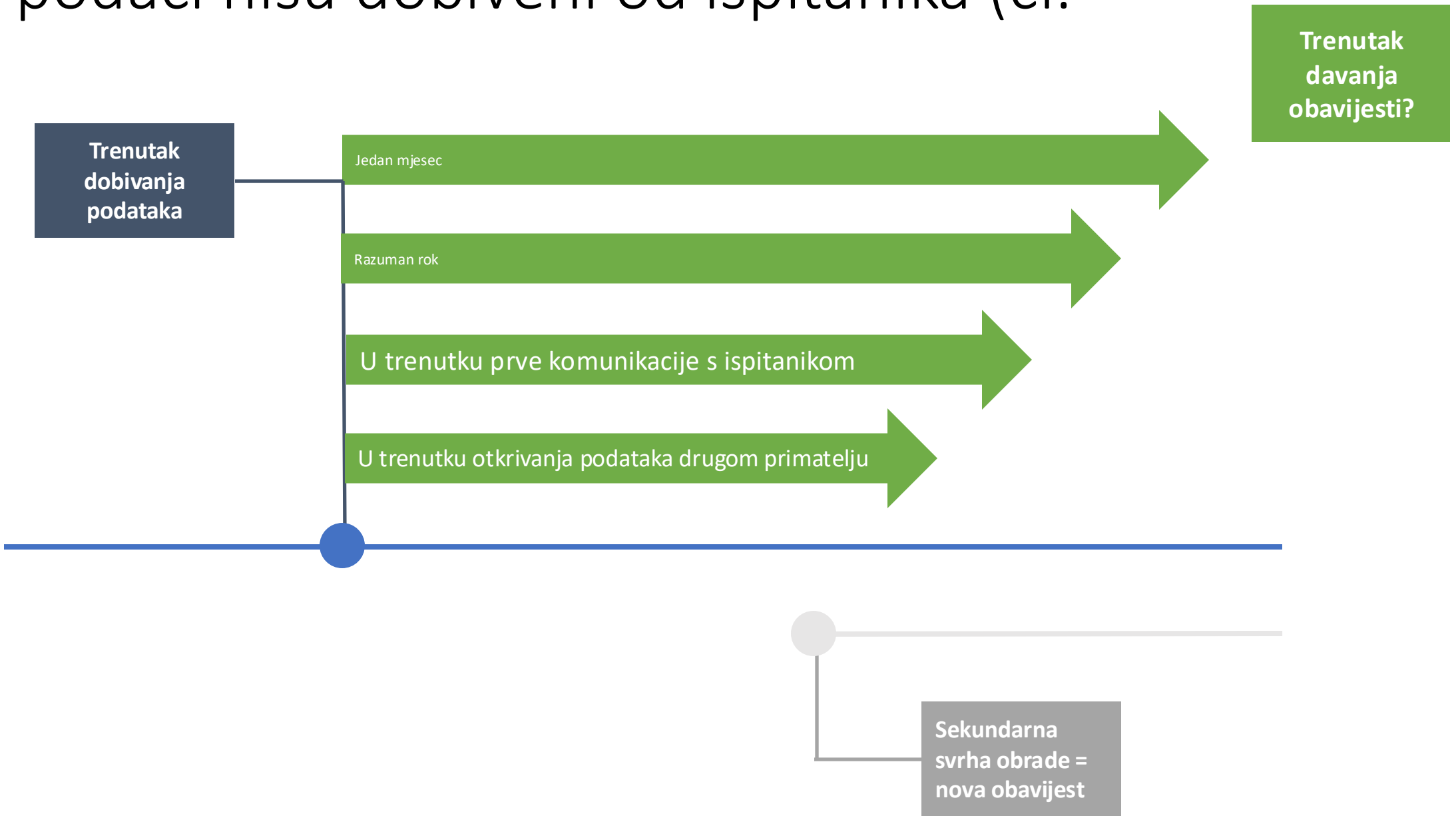


Iznimka

(1) ako ispitanik već raspolaže informacijama

(2) u onoj mjeri u kojoj ispitanik već raspolaže informacijama

Ako podaci nisu dobiveni od ispitanika (čl. 14.)



Ako podaci nisu dobiveni od ispitanika (čl. 14.)

Iznimka

(1) ako ispitanik već raspolaže informacijama

(2) u onoj mjeri u kojoj ispitanik već raspolaže informacijama

Pravo ispitanika na pristup

Pravo ispitanika na pristup podacima (čl. 15.)

Dobiti informaciju obrađuju li se podaci koji se odnose na njega	Dobiti pristup podacima i informacijama o obradi	Dobiti kopiju podataka
DA / NE	Pristup podacima Informacije o obradi: svrha, kategorije podataka, primatelji, razdoblje čuvanja, obavijest o pravima, izvor podataka, logika automatske obrade… + zaštitne mjere u slučaju izvoza podataka	Prva kopija BEZ NAKNADE (čl. 12/5, čl. 15/3) Dodatne kopije = razumna naknada troškova Ako je zahtjev elektronički, informacije se pružaju u „uobičajenom elektroničkom obliku” (mail, web sučelje, …) Negativan utjecaj na prava drugih

Pravo ispitanika na pristup podacima – recital 63

Ispitanik bi trebao imati pravo pristupa prikupljenim osobnim podacima koji se na njega odnose te ostvarivati to pravo lako i u razumnim intervalima **kako bi bio svjestan obrade i provjerio njezinu zakonitost**. To uključuje pravo ispitanika na pristup podacima o njegovom zdravstvenom stanju, na primjer podacima u medicinskoj dokumentaciji koja sadržava informacije poput dijagnoza, rezultata pretraga, liječničkih mišljenja, liječenja ili zahvata. Svaki ispitanik stoga bi osobito trebao imati pravo znati i dobiti obavijest o svrhama obrade osobnih podataka, ako je moguće i za koje razdoblje se osobni podaci ….

Pravo ispitanika na ispravak podataka

Pravo na ispravak podataka

Ispravak netočnih podataka

- Činjenice / mišljenja
- Ispitanik dokazuje netočnost informacije

Dopuna nepotpunih podataka

- Samo ako je dopuna podataka bitna za svrhu obrade i ako je njeno izvršenje proporcionalno cilju

Pravo na brisanje podataka

Pravo na brisanje podataka

Razlozi za brisanje	Pravo na brisanje ne primjenjuje se ako je obrada nužna:
(a) osobni podaci više nisu nužni u odnosu na svrhu (b) ispitanik povuče privolu (i ako ne postoji druga pravna osnova za obradu) (c) ispitanik uloži prigovor na obradu u skladu s člankom 21. stavkom 1. te ne postoje jači legitimni razlozi za obradu, ili ispitanik uloži prigovor na obradu u skladu s člankom 21. stavkom 2.; (d) osobni podaci nezakonito su obrađeni; (e) osobni podaci moraju se brisati radi poštovanja pravne obveze iz prava Unije ili prava države članice kojem podliježe voditelj obrade; (f) osobni podaci prikupljeni su u vezi s ponudom usluga informacijskog društva iz članka 8. stavka 1.	(a) radi ostvarivanja prava na slobodu izražavanja i informiranja; (b) radi poštovanja pravne obveze kojom se zahtijeva obrada u pravu Unije ili pravu države članice kojem podliježe voditelj obrade ili za izvršavanje zadaće od javnog interesa ili pri izvršavanju službene ovlasti voditelja obrade; (c) zbog javnog interesa u području javnog zdravlja u skladu s člankom 9. stavkom 2. točkama (h) i (i) kao i člankom 9. stavkom 3.; (d) u svrhe arhiviranja u javnom interesu, u svrhe znanstvenog ili povijesnog istraživanja ili u statističke svrhe u skladu s člankom 89. stavkom 1. u mjeri u kojoj je vjerojatno da se pravom iz stavka 1. može onemogućiti ili ozbiljno ugroziti postizanje ciljeva te obrade; ili (e) radi postavljanja, ostvarivanja ili obrane pravnih zahtjeva.

Pravo na ograničenje obrade

Pravo na ograničenje obrade

Razlozi za ograničenje obrade	Posljedice ograničenja obrade
(a) ispitanik osporava točnost osobnih podataka, na razdoblje kojim se voditelju obrade omogućuje provjera točnosti osobnih podataka; (b) obrada je nezakonita i ispitanik se protivi brisanju osobnih podataka te umjesto toga traži ograničenje njihove uporabe; (c) voditelj obrade više ne treba osobne podatke za potrebe obrade, ali ih ispitanik traži radi postavljanja, ostvarivanja ili obrane pravnih zahtjeva; (d) ispitanik je uložio prigovor na obradu na temelju članka 21. stavka 1. očekujući potvrdu nadilaze li legitimni razlozi voditelja obrade razloge ispitanika.	2. Ako je obrada ograničena stavkom 1., takvi osobni podaci smiju se obrađivati samo uz privolu ispitanika, uz iznimku pohrane, ili za postavljanje, ostvarivanje ili obranu pravnih zahtjeva ili zaštitu prava druge fizičke ili pravne osobe ili zbog važnog javnog interesa Unije ili države članice. 3. Ispitanika koji je ishodio ograničenje obrade na temelju stavka 1. voditelj obrade izvješćuje prije nego što ograničenje obrade bude ukinuto.

Pravo na prenosivost podataka

Korisni izvori

- **Što se prenosi?**
  - Podaci koje je ispitanik pružio voditelju obrade u strukturiranom, uobičajeno upotrebljavanom i strojno čitljivom formatu
- **Subjektivno pravo ispitanika:**
  - Zaprimiti takve podatke
  - Prenijeti ih drugom voditelju obrade bez ometanja od strane prvog
  - Izravni prijenos od jednog voditelja obrade drugome ako je to tehnički izvedivo

Pravo na prigovor

Pravo na prigovor

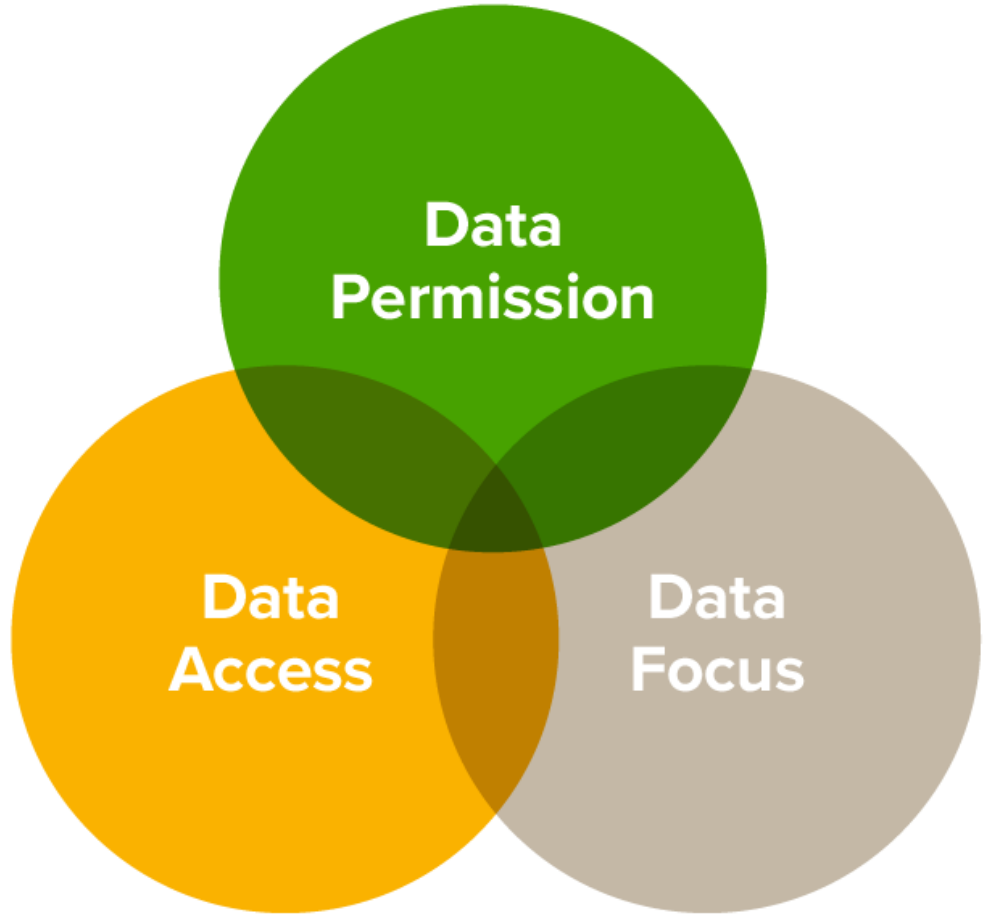
Ispitanik ima pravo na temelju svoje posebne situacije u svakom trenutku uložiti prigovor na obradu osobnih podataka koji se odnose na njega, u skladu s člankom 6. stavkom 1. točkom (e) ili (f), uključujući izradu profila koja se temelji na tim odredbama. Voditelj obrade više ne smije obrađivati osobne podatke osim ako voditelj obrade dokaže da postoje uvjerljivi legitimni razlozi za obradu koji nadilaze interese, prava i slobode ispitanika ili radi postavljanja, ostvarivanja ili obrane pravnih zahtjeva.

Pravo na prigovor

1. Općenito: Prigovor na obradu temeljenu na legitimnim interesu ili izvršavanju zadaće od javnog interesa ili pri izvršavanju službene ovlasti voditelja obrade > voditelj mora dokazati da postoje prevladavajući razlozi za obradu
2. U slučaju marketinga, uključujući profiliranje > prestanak obrade

GDPR & Markting

GDPR and Marketing



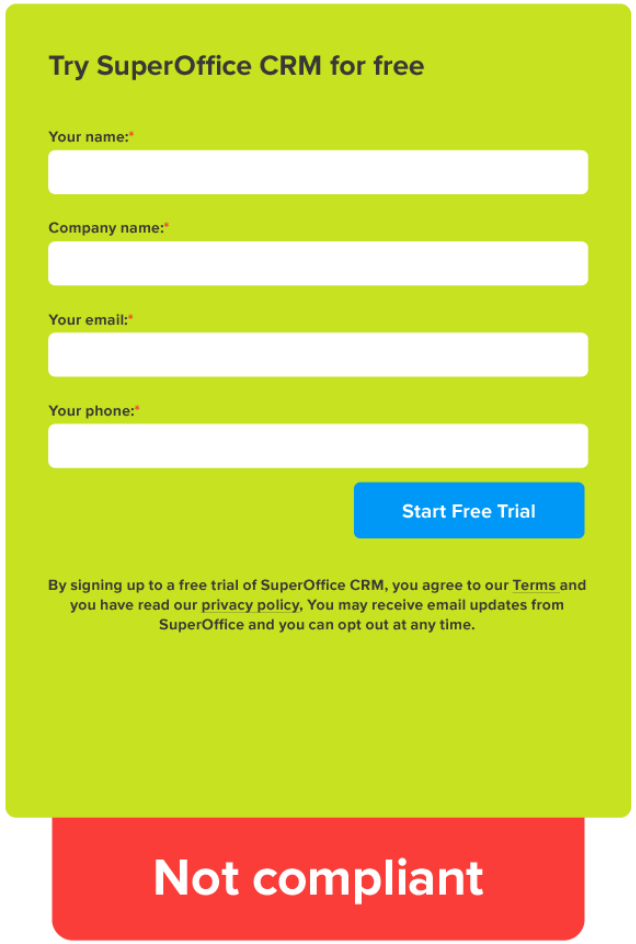
Data Permission

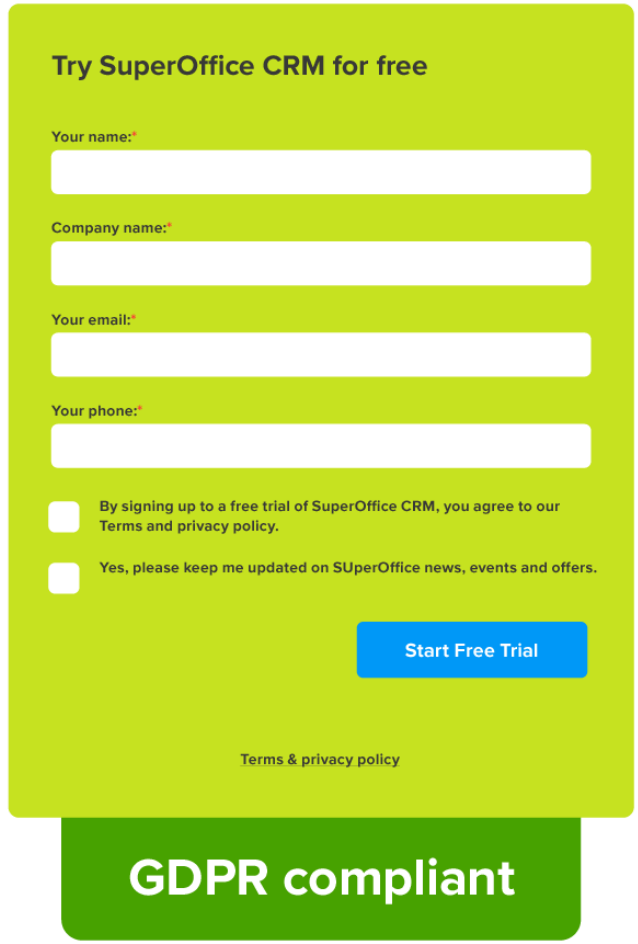
- Dopuštenje za podatke odnosi se na način na koji upravljate prijavama putem e-pošte – osobama koje od vas traže da primaju promotivni materijal.

- Ne možete pretpostaviti da žele biti kontaktirani. Ubuduće moraju izraziti pristanak na "slobodno dan, specifičan, informiran i nedvosmislen" način, koji je pojačan "jasnom afirmativnom radnjom".

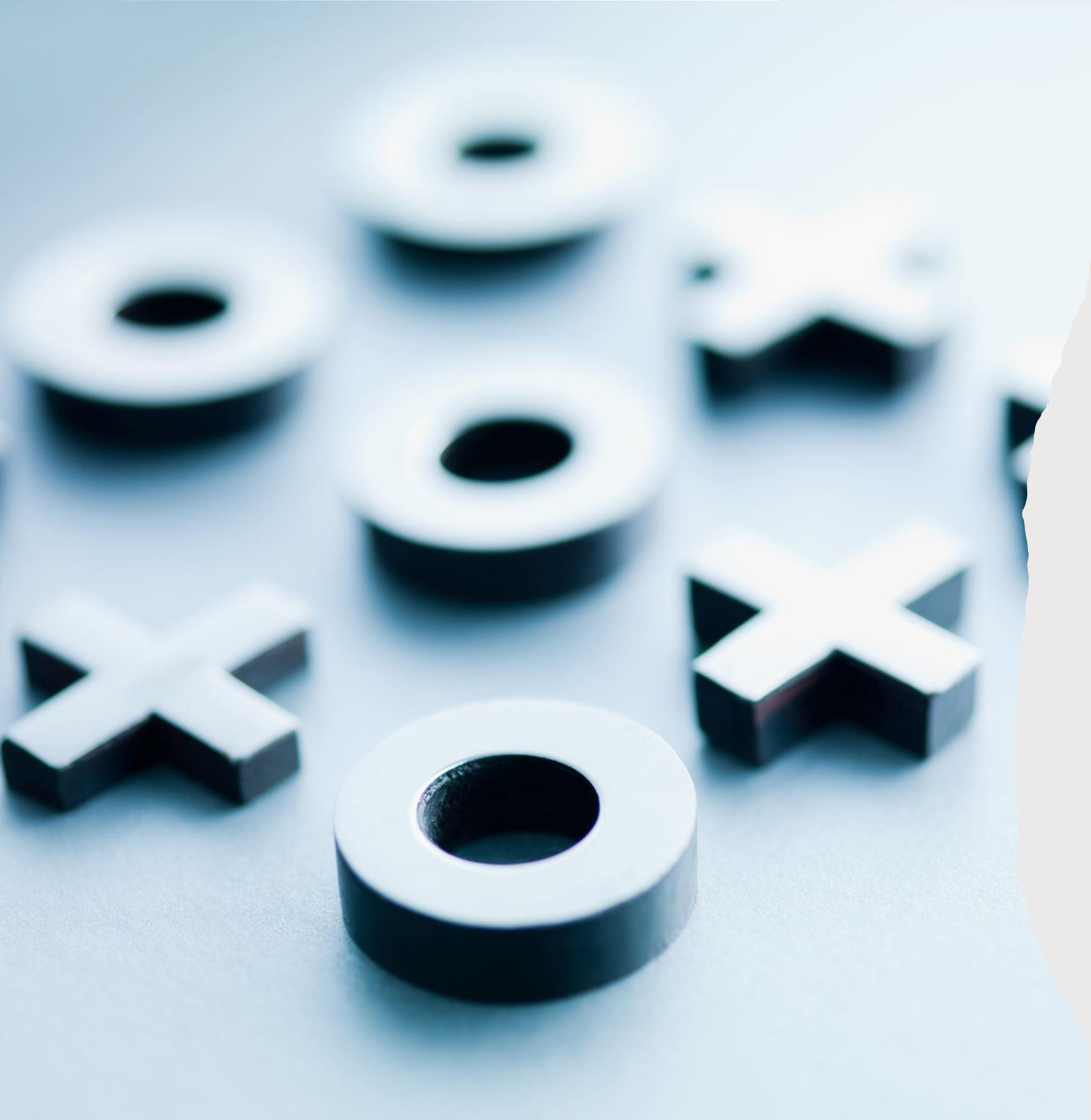
- To znači da potencijalni klijenti, kupci i partneri, moraju fizički potvrditi da žele biti kontaktirani. Morate biti sigurni da ste aktivno tražili (a ne pretpostavljali) dopuštenje od svojih potencijalnih kupaca i klijenata, potvrđujući da žele da ih se kontaktira. Stoga, unaprijed označeni okvir koji ih automatski uključuje više neće smetati - uključivanje mora biti namjeran izbor.

Primjer privole





Na primjer, umjesto pretpostavke da posjetitelji koji ispune web obrazackojim žele primati marketinšku e-poštu od SuperOfficea (lijevo), sada tražimo od posjetitelja da se posebno odluče za primanje biltena označavanjem okvira za prijavu (desno).



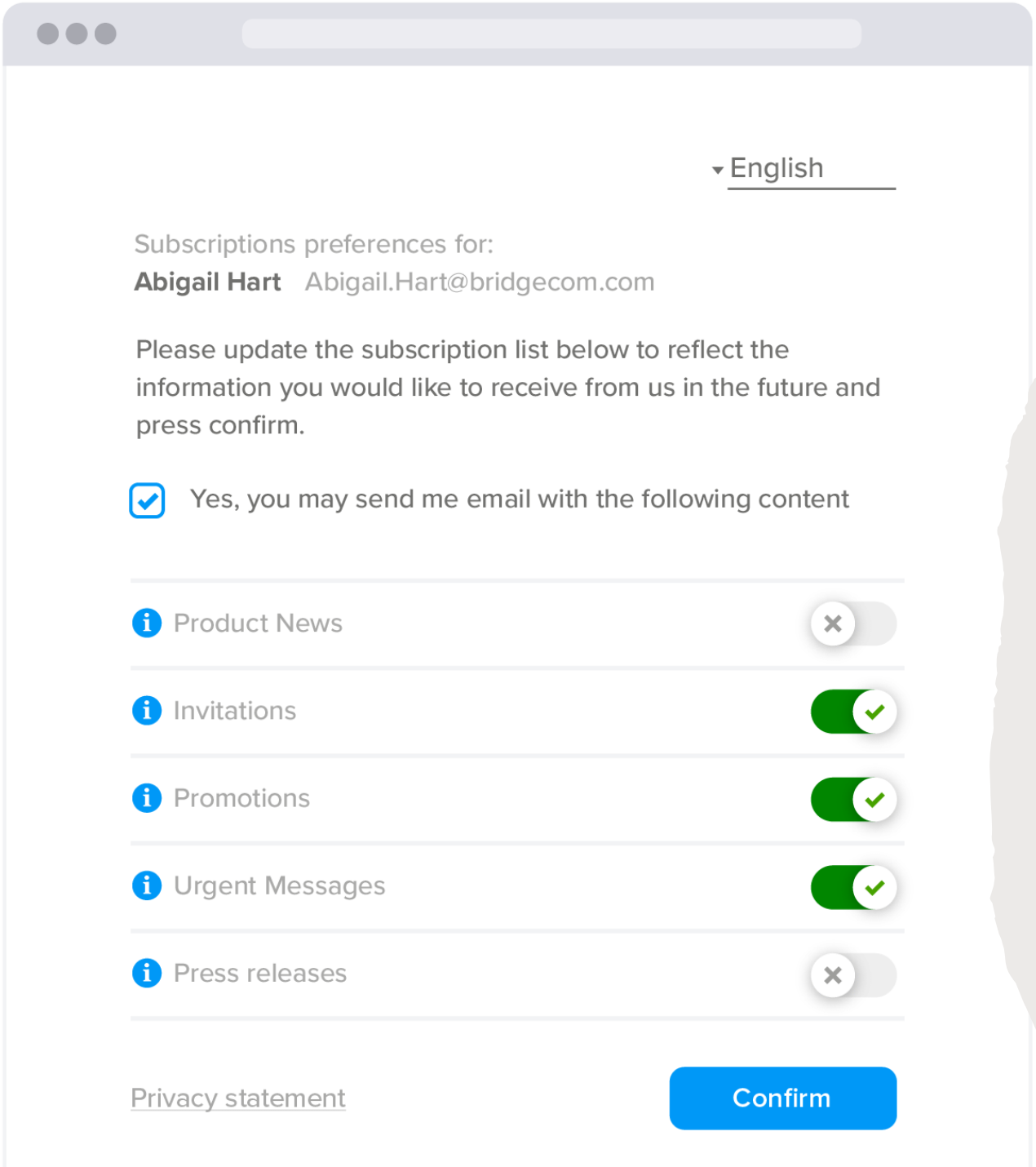
Data Access

- Pravo na zaborav postalo je nešto čemu se najviše govorilo u povijesti Suda pravde EU-a.

- Daje ljudima pravo na uklanjanje zastarjelih ili netočnih osobnih podataka, a u nekim slučajevima već su ga primijenile tvrtke poput Googlea, koje su bile prisiljene ukloniti stranice iz rezultata svoje tražilice kako bi se pridržavale zahtjeva.

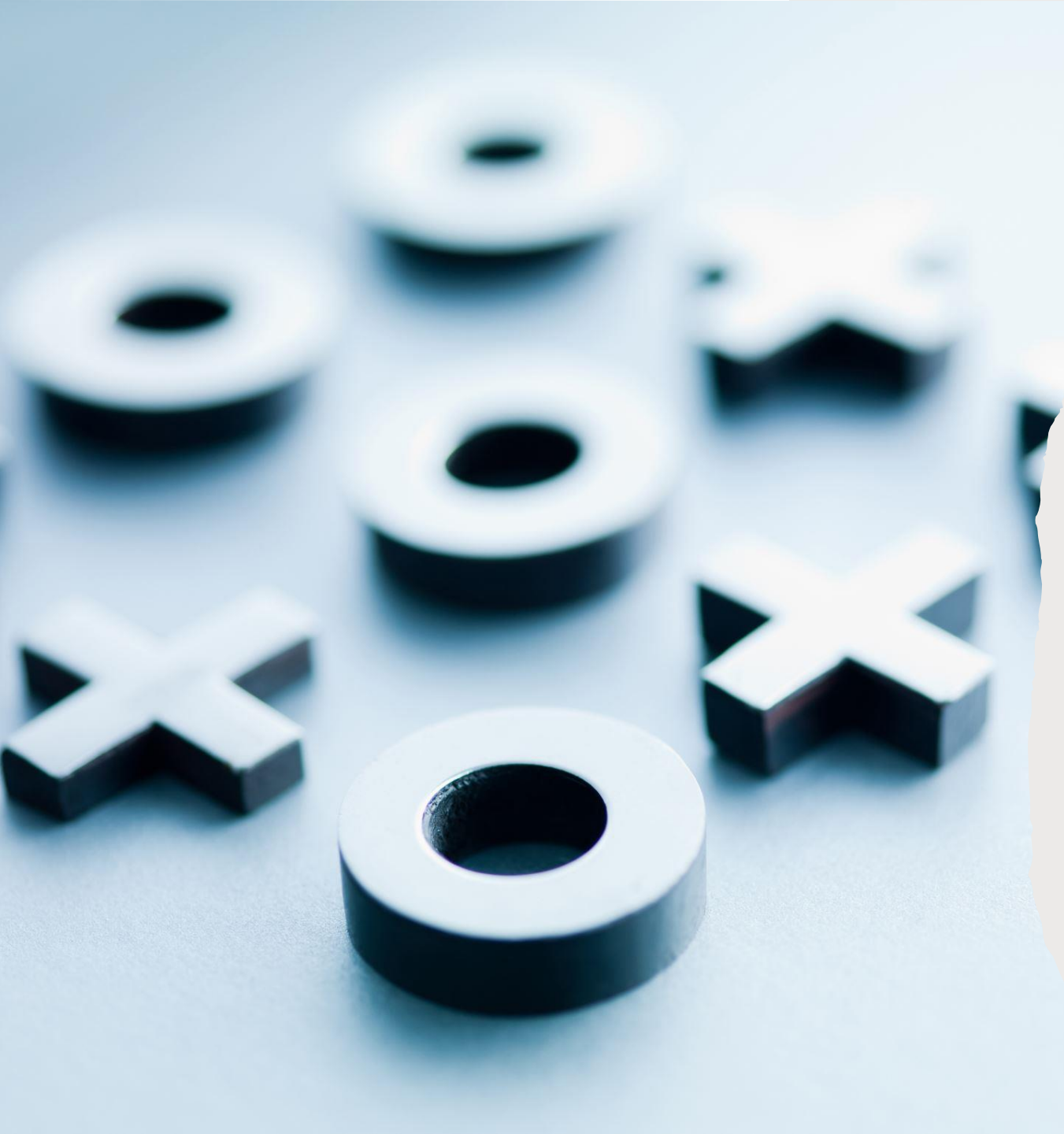
- Uvođenje GDPR-a nudi pojedincima metodu za stjecanje veće kontrole nad načinom na koji se njihovi podaci prikupljaju i koriste – uključujući mogućnost pristupa ili uklanjanja istih – u skladu s njihovim pravom na zaborav.

- Kao trgovac, bit ćete odgovorni osigurati da vaši korisnici mogu lako pristupiti svojim podacima i ukloniti privolu za njihovu upotrebu.



Pristup podacima

- Praktično govoreći, to može biti jednostavno poput uključivanja veze za odjavu pretplate unutar vašeg marketinškog predloška putem e-pošte i povezivanja s profilom korisnika koji korisnicima omogućuje upravljanje postavkama e-pošte (kao što je prikazano u primjeru).



Data focus – fokus je na podacima

- Kao marketinški stručnjaci, svi možemo biti krivi za prikupljanje malo više podataka od osobe nego što nam je zapravo potrebno.

- Zapitajte se trebam li doista znati nečiji omiljeni film prije nego što se pretplati na naš newsletter?

- Imajući to na umu, GDPR zahtijeva da pravno opravdate obradu osobnih podataka koje prikupljate.

- To znači da se trebate usredotočiti na podatke koji su vam potrebni i prestati tražiti ono što je “dobro imati”. Ako stvarno trebate znati broj cipela za posjetitelje i možete dokazati zašto vam je to potrebno, možete nastaviti to i tražiti. U protivnom pokušajte izbjeći prikupljanje nepotrebnih podataka i držite se osnova.

Naputak za marketing 1/3

- **Pregledajte svoju mailing listu**
  - Za nove pretplatnike, pobrinite se da potencijalni pretplatnik potvrdi da se on ili ona želi pridružiti vašoj listi za slanje e-pošte slanjem automatske e-pošte za potvrdu pretplate.

- **Pregledajte način na koji prikupljate osobne podatke**
  - JD Whetherspoon poduzeo je korak bez presedana i izbrisao cijelu bazu podataka o marketingu e-pošte (više od 650.000 adresa e-pošte)

- **Uložite u content marketing strategiju**
  - stvaranjem white papers, vodiča i e-knjiga kojima posjetitelji mogu pristupiti i preuzeti ih u zamjenu za dijeljenje svojih podataka za kontakt.

- **Educirajte svoj prodajni tim o novim tehnikama prodaje**
  - U suštini, prodajni predstavnici trebali bi se povezati s potencijalnim kupcima na društvenim medijima i dijeliti relevantan sadržaj - umjesto da pokušavaju doći do novih potencijalnih klijenata putem e-pošte. Uložite u strategije kao što su socal selling i account-based marketing.

Naputak za marketing 2/3

- **Počnite centralizirati svoje prikupljanje osobnih podataka u CRM sustav**
  - Vrijeme korištenja Google dokumenata ili Excel proračunskih tablica za pohranu podataka o kupcima je prošlo. I pobrinite se da vaši korisnici mogu pristupiti svojim podacima, pregledati njihovu predloženu upotrebu i izvršiti sve potrebne promjene.

- **Detaljnije shvatite podatke koje prikupljate**
  - Je li sve to potrebno ili postoje elementi bez kojih se može? Kada je riječ o obrascima za prijavu, tražite samo ono što vam je potrebno i što ćete koristiti. Za B2B trgovce, puno ime, adresa e-pošte i naziv tvrtke obično su više nego dovoljni.

- **Pozovite posjetitelje da se dodaju na vaš popis za slanje e-pošte pokretanjem pop-up prozora na vašoj web stranici**
  - Svoj popis za slanje e-pošte možete održavati uredno segmentiranim stvaranjem posebnih skočnih prozora za vijesti o proizvodima, postove na blogu i općenite vijesti o tvrtki. Samo se ne zaboravite povezati sa svojim pravilima o privatnosti kako biste osigurali usklađenost.

Naputak za marketing 3/3

- **Pokušajte koristiti push obavijesti**
  - Push notification je skočna poruka koja se pojavljuje na stolnom računalu ili mobilnom uređaju. Marketinški stručnjaci mogu koristiti push obavijesti za slanje poruke pretplatnicima u bilo kojem trenutku. Međutim, za razliku od marketinških kampanja putem e-pošte, push obavijesti ne obrađuju osobne podatke (IP adrese su anonimizirane) i korisnici moraju dati izričit pristanak kako bi se uključili i primali obavijesti.

- **Ažurirajte svoju izjavu o privatnosti**
  - Pregledajte svoju trenutnu izjavu o privatnosti i izmijenite je u skladu sa zahtjevima GDPR-a. Je li teško pročitati sadržaj vaše izjave o privatnosti? Ili namjerno koristite terminologiju kako potencijalni kupci ne bi znali na što se upisuju? Ako je tako, prepišite je i učinite lakim za čitanje.

Influenceri

1. Kod kontaktiranja influencera. koja je uloga klijenta, a koja agencije?

- Klijent je po pitanju obrade podataka definiran kao voditelj obrade podataka, dok je agencija izvršitelj obrade.

2. Koje podatke influencera smijem prikupljati?

- U svrsi direktne poslovne komunikacije smijete prikupiti one podatke koje vam je influencer osobno dao iii podatke koji su javno dostupni, tako da se može zaključiti kako su dani radi poslovnog kontaktiranja. Kontaktiranje influencera i komunikacija s njime može predstavljati legitimni interes. Daljnja obrada može predstavljati ugovorenu obvezu.

3. Koliko različitih privola smijem tražiti od influencera istovremeno?

- Nema ograničenja, ali se provodi načelo nužnosti: dakle, samo one podatke koji su nužni za doseg određenog cilja.

4. Što ako mi Influencer pošalje da ne želi da se njegovi podaci koriste nadalje?

- Nećete koristiti podatke ako su prikupljeni temeljem privole ili je prestala svrha obrade, kao i kod svakog drugog ispitanika.

5. Smijem li koristiti podatke koje mi Je influencer sam poslao preko Facebook/Instagram inboxa ili javno?

Da, ako vam je sam poslao u svrhu daljnje komunikacije. Javna objava opisana je prethodno.

6. Smijem li kontaktirati influencera preko Facebook/Instagram inboxa iii javnog emaila navedenog na profilu?

Da.

7. Smijem II samoinicijativno sherati objavu influencera?

Samo unutar originalne platforme na kojoj je sadržaj objavljen.

8. Što ako radimo kampanju u kojoj Influencer skuplja podatke dobitnika natječaja?

Ako influencer prikuplja osobne podatke, potrebno je da to radi onako kako propisuje voditelj obrade (klijent). Drugim riječima, treba potpisati ugovor s izvršiteljem obrade (agencijom) i izvršiti sve korake koji su potrebni da bi se osiguralo da se izvođenje obrade podataka vrši prema Uredbi i Zakonu. U praksi treba nastojati to izbjeći tako da mehanika kampanje osigurava da izvršitelj obrade bude agencija, a ne influencer.

Nagradne igre

Kako ne bi bilo zabune vezane za značenje nagradnih igara u različitim okolnostima, svakako treba imati na umu da su nagradne igre u okviru provođenja igara na sreću definirane Pravilnikom o priređivanju nagradnih igara Ministarstva financija.

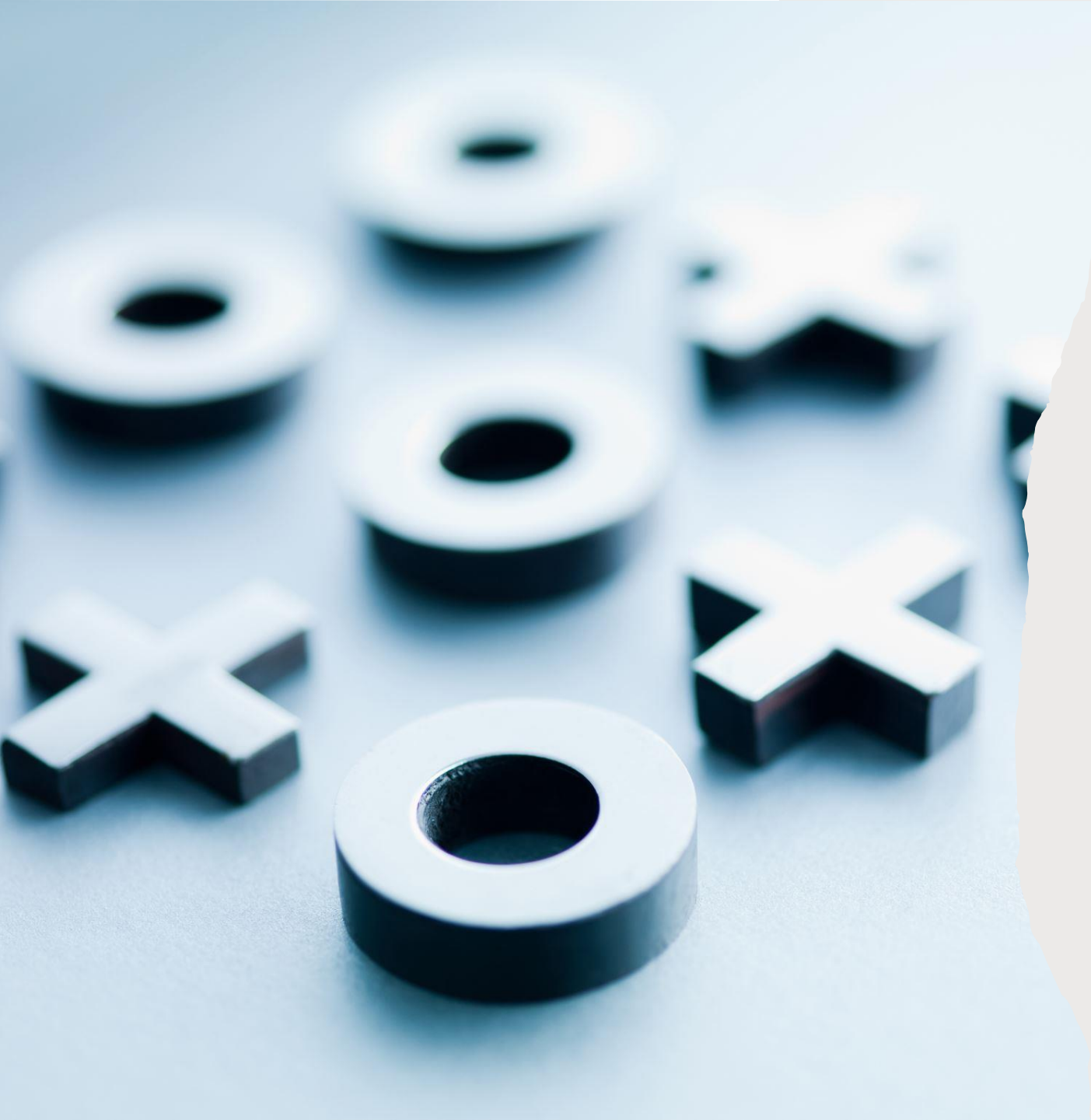
Nagradna igra jest igra koju radi promidžbe svojih proizvoda i usluga priređuju trgovačka društva te druge pravne i fizičke osobe poduzetnici, pri čemu se priređivač obvezuje izvučenim dobitnicima podijeliti nagrade u robi ili uslugama, a da se od sudionika ne zahtijeva posebna uplata za sudjelovanje u nagradnoj igri.

1. Koja je uloga klijenta, a koja agencije kod organizacije natječaja iii igre?

Klijent je priređivač, dakle nositelj i organizator natječaja ili igre. Agencija provodi natječaj ili igru za klijenta kao podizvođač, a takvi odnosi trebaju biti regulirani ugovorom. Prema tome, klijent je po pitanju obrade podataka definiran kao voditelj obrade podataka, dok je agencija Izvršitelj obrade.

2. Koje podatke korisnika smijem prikupljati kroz nagradni natječaj/igru?

One podatke koji su nužni kako bi se natječaj/igra proveo/la (aktivnost koja je predstavljena kao cilj održavanja nagradnog natječaja/Igre), odnosno oni podaci koju su regulirani zakonom. Primjerice: dostava nagrada, istraživanje ciljne skupine i/ili navika potrošača, građenje newsletter baze i slično. Smiju se prikupljati oni podaci koji su zaista nužni za predstavljeni cilj. Dakle, korisnike se ne može pitati za primjerice dob, ako to nije opravdano ciljem nagradnog natječaja/igre.



3. Smijem li se korisniku javiti preko Facebooka/Instagrama kako bih skupio podatke?

Da, kontaktiranje fanova je dozvoljeno kroz Facebook/Instagram platformu ako se radi o komunikaciji koja je u svrhu dostave nagrade ili ako je propisano pravilima nagradne igre. I dalje vrijedi načelo da se podaci ne smiju koristiti u druge svrhe.

4. Smijem li koristiti podatke koje mi je korisnik sam poslao preko inboxa Facebooka/Instagrama ili javno?

Ako se radi o svrsi koja je definirana i komunicirana korisniku, kao što je to, na primjer, legitimni interes vezan za dostavu nagrade ili komunikacija koja je bila navedena u okviru pravila nagradne igre, da. I dalje vrijedi načelo da se podaci ne smiju koristiti u druge svrhe.

5. Smijem li koristiti user generated content za promociju natječaja?

Podaci koji su prikupljeni u svrhu provođenja nagradne igre ili natječaja definirani pravilima nagradne igre ili natječaja, mogu se koristiti u svrhu provođenja nagradne igre ili natječaja, osim u slučaju da su za vrijeme prikupljanja sudionici privolom dali dozvolu za neku drugu svrhu.

6. Što ako mi netko od Sudionika pošalje da ne želi da se njegovi podaci koriste u Natječaju (izjava, ime...)?

Ako je sudionik prihvatio sudjelovanje u nagradnoj igri, pri čemu su mu bila dostupna pravila nagradne igre, temelj za obradu vezan je za ta pravila.

7. Smijem li kao tvrtka koristiti podatke korisnika iz natječaja ili igre za potrebe najave drugog natječaja ili igre?

Ne, osim ako se prilikom prikupljanja podataka nije provela i privola za neke druge svrhe različite od same nagradne igre iii natječaja.

10. Mora li se u pravilima natječaja/igre navesti svaku svrhu korištenja podataka zasebno?

Svrha u okviru pravila nagradne igre može biti isključivo vezana za provođenje nagradne igre. Preporuka je transparentno opisati svrhu, opise podataka i vremena čuvanja u okviru takvih pravila.

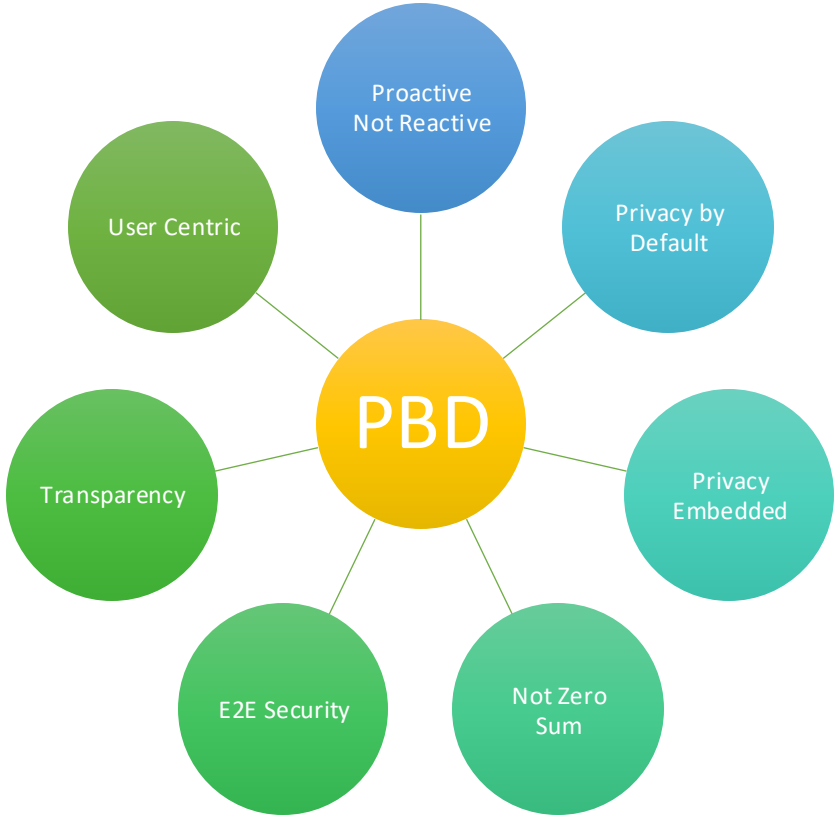
11. Smijem II javno objaviti imena dobitnika nagradnog natječaja ili igre?

Sukladno pravilima nagradne igre ili natječaja.

Ostalo

Privacy by Design

Koncept integrirane zaštite privatnosti (Privacy by Design) odnosi se na neophodnost integriranja privatnosti i zaštite osobnih podataka u informacijsko komunikacijskoj tehnologiji od početka do kraja njihovog životnog ciklusa: od faze koncepcije (dizajna) do izlaska iz upotrebe.



Prijava povrede osobnih podataka

GDPR uključuje prijavu povrede osobnih podataka:

- *voditelju obrade (ukoliko ste izvršitelj obrade podataka)*
- *nadzornom tijelu*
- *pogođenim pojedincima - vlasnicima osobnih podataka*

Trenutno ne postoje pravila na razini EU
(osim telco i ISP)

- izvještaj se očekuje u roku 72 sata

Imenovanje DPO

Postavljanje Službenika za zaštitu osobnih podataka – DPO (Data Protection Officer)

- kako za izvršitelje obrade tako i za voditelje obrade
- *Može biti zaposlen ili eksternaliziran*

- *Prag za imenovanje:*
  - *obavezno za tvrtke s javnim ovlastima*
  - *sistematski nadzor pojedinaca i osobnih podataka na **velikoj skali***
  - *obrada osjetljivih podataka na **velikoj skali***
  - *obaveza za tvrtke iznad 250 zaposlenih*

Poslovi:

- *podrška, informiranje i savjetovanje*
- *nadzire usklađenost*
- *svijest/edukacija*
- *obavlja PIA, PII Data Discovery*
- *točka kontakta*
- *uključen u sve slučajeve*
- *odgovoran Upravi*

Dizanje svijesti

Edukacija vanjskih partnera, izvršitelja, dobavljača i djelatnika

1. stvaranje preduvjeta
2. revizija postojećih procedura i dokumentacije
3. čišćenje postojećih baza osobnih podataka i revizija prava
4. definiranje novih pravila
5. implementacija novih rješenja i nadogradnja postojećih
6. **dizanje svijesti**

Prva kazna za kršenje GDPR-a u Hrvatskoj bit će veća od 100.000 kn

U objavi o donošenju rješenja AZOP je tad naveo da je od jedne banke čak 34 puta tražio da se uskladi s GDPR regulativom.

Prva novčana kazna za kršenje GDPR regulative u Hrvatskoj bit će veća od 100.000 kuna, doznaje Poslovni dnevnik.

Sredinom ožujka Agencija za zaštitu osobnih podataka (AZOP) objavila je da je donijela prvo takvo rješenje, ali i oko njega stvorila misteriju jer nije navela iznos kazne, ime subjekta koji je kaznila kao ni da nije objavila samo rješenje.

Kazne

azop Agencija za zaštitu osobnih podataka

O AZOP-U DOKUMENTI GRAĐANI VODITELJI I IZVRŠITELJI OBRADE SLUŽBENIK ZA ZAŠTITU PODATAKA

Rješenje kojim se izriče upravno novčana kazna zbog odbijanja dostave osobnih podataka ispitanicima

ZAHT

azop Agencija za zaštitu osobnih podataka

O AZOP-U DOKUMENTI GRAĐANI VODITELJI I IZVRŠITELJI OBRADE SLUŽBENIK ZA ZAŠTITU PODATAK

Izdana nova upravna novčana kazna

22. 2. 2021.

ZAH

Zaštitarskoj tvrtki 500.000 kuna kazne za video muškarca koji se križao nakon dezinficiranja ruku

To je prvenstveno poruka voditeljima i izvršiteljima obrade da se Opća uredba o zaštiti podataka mora shvatiti ozbiljno, govore iz Agencije

Izrečene dvije upravne novčane kazne u ukupnom iznosu 2,18 milijuna kuna

21. srpnja 2022.

Upravna novčana kazna od 2.15 milijun kuna zbog nepoduzimanja odgovarajućih tehničkih i organizacijskih mjera

Agencija za zaštitu osobnih podataka izrekla je upravnu novčanu kaznu u iznosu od 2,15 milijuna kuna voditelju obrade – pružatelju telekomunikacijskih usluga zbog nepoduzimanja odgovarajućih tehničkih i organizacijskih mjera sigurnosti obrade osobnih podataka, što je dovelo do neovlaštene obrade osobnih podataka cca 100.000 ispitanika, odnosno neovlaštenog pristupa osobnim podacima od strane napadača. Voditelj obrade nije poduzeo potrebne mjere za postizanje odgovarajuće mjere sigurnosti sukladno postojećim predvidivim rizicima, čime je postupio protivno članku 25. stavku 1. te članku 32. stavku 1. točke b) i d) i stavku 2. Opće uredbe o zaštiti podataka.

Izrečene upravne novčane kazne u ukupnom iznosu od 1.6 milijuna kuna

8.3.2022.

Upravna novčana kazna zbog nedostavljanja kopije osobnih podataka na zahtjev ispitanika

Agencija za zaštitu osobnih podataka izrekla je upravnu novčanu kaznu u iznosu od 940.000,00 kuna voditelju obrade odnosno društvu iz područja energetskog sektora (u daljnjem tekstu: Društvo) zbog nedostavljanja snimki videonadzornih kamera (kopije osobnih podataka) na zahtjev ispitanika, čime je došlo do **povrede članka 15. stavka 3. Opće uredbe o zaštiti podataka.**

Upravna novčana kazna od 30 tisuća kuna zbog neoznačavanja objekta pod videonadzorom

Agencija za zaštitu osobnih podataka je po službenoj dužnosti, bez prethodne najave, provela izravan nadzor nad obradom i provođenjem zaštite osobnih podataka, prikupljanja i obrade osobnih podataka učinjenih videonadzornim sustavom te je utvrdila kako voditelj obrade – prodajno-servisni centar automobila sa sjedištem u Zagrebu nije označio da su pojedine prostorije u njemu, kao i vanjske površine predmetnog objekta, pod videonadzorom, a što je protivno članku 27. stavku 1. Zakona o provedbi Opće uredbe o zaštiti podataka.

Upravna novčana kazna zbog nepoduzimanja odgovarajućih mjera sigurnosti obrade osobnih podataka

Agencija za zaštitu osobnih podataka izrekla je upravnu novčanu kaznu u iznosu od 675.000,00 kuna zbog nepoduzimanja odgovarajućih mjera sigurnosti obrade osobnih podataka od strane trgovačkog lanca (u daljnjem tekstu: Društvo) kao voditelja obrade, **protivno članku 32. stavku 1. točke b) i d) te stavku 2. i 4. Opće uredbe o zaštiti podataka** što je dovelo do neovlaštene obrade osobnih podataka ispitanika njihovom javnom objavom na društvenim mrežama i u medijima.

Agencija za zaštitu osobnih podataka (AZOP) izdala je zbog kršenja odredbi Opće uredbe o zaštiti podataka-GDPR i zakona o provedbi te uredbe od 2020. do sada 32 upravne novčane kazne u ukupnom iznosu od 3,1 milijun eura, od čega samo od početka godine 13 kazni u visini od 2,3 milijuna eura.

U tih 13 izrečenih kazni od početka ove godine uključena je i najnovija, izrečena agenciji za naplatu potraživanja B2 Kapital u iznosu od 2,26 milijuna eura uslijed kršenja više odredbi Opće uredbe o zaštiti podataka-GDPR, naveli su iz AZOP-a za Hinu.

Ta je kazna ujedno i najveća do sada izrečena za kršenje odredbi te uredbe u pet godina od početka njezine primjene.

Inače, pet godina primjene uredbe GDPR navršava se 25. svibnja 2023., a tim će se povodom u EU iznova promovirati i isticati važnost primjene te uredbe o zaštiti osobnih podataka.

Sportskoj kladionici izrečena upravna novčana kazna od 380.000 eura

Agencija za zaštitu osobnih podatka izrekla je **upravnu novčanu kaznu voditelju obrade** – trgovačkom društvu za priređivanje igara na sreću – igara klađenja **(sportskoj kladionici) u iznosu od 380.000,00 eura** zbog sljedeće utvrđenih povreda Opće uredbe o zaštiti podataka:

1. **Voditelj obrade obrađivao je osobne podatke odnosno preslike bankovnih kartica ispitanika, a za čiju obradu nije dokazana pravna osnova** čime je povrijeđen članak 6. stavak 1. Opće uredbe o zaštiti podataka;
2. **Voditelj obrade nije na adekvatan način obavijestio ispitanike** o obradi osobnih podataka, odnosno **o obradi podataka sadržanim na preslikama bankovnih kartica**, čime je povrijeđen članak 13. stavak 1. i 2. Opće uredbe o zaštiti podataka;
3. Prilikom kreiranja novog poslovnog procesa za uslugu brze isplate na VISA bankovnu karticu, **voditelj obrade nije implementirao odgovarajuće tehničke i organizacijske mjere**, čime je povrijeđen članak 25. stavak 1. i 2. Opće uredbe o zaštiti podataka;
4. **Voditelj obrade nije primjenjivao tehničku mjeru enkripcije na osobne podatke ispitanika pohranjene u bazama podataka** voditelja obrade te **nije redovno procjenjivao učinkovitosti tehničkih i organizacijskih mjera** za osiguravanje sigurnosti obrade, a čime je povrijeđen članak 32. stavak 1. točka a) i d) Opće uredbe o zaštiti podataka.

Agenciji za naplatu potraživanja EOS Matrix d.o.o. izrečena upravna novčana kazna u iznosu od 5,47 milijuna eura

5. listopada 2023.

Agencija za zaštitu osobnih podataka izrekla je **upravnu novčanu kaznu u iznosu od 5.470.000,00 eura (41.213.715,00 kuna) EOS Matrix d.o.o.** kao voditelju obrade zbog sljedeće utvrđenih povreda Opće uredbe o zaštiti podataka:

1. Voditelj obrade **nije poduzeo odgovarajuće tehničke mjere** zaštite obrade osobnih podataka ispitanika sadržanih u sustavima pohrane, a što je protivno članku 32. stavku 1. točke b) i stavku 2. Opće uredbe o zaštiti podataka.
2. Voditelj obrade **obrađivao je osobne podatke ispitanika koji nisu u dužničko-vjerovničkom odnosu** u svojoj bazi (aplikaciji) **bez postojanja pravne osnove** iz članka 6. stavka 1. Opće uredbe o zaštiti podataka
3. Voditelj obrade je **obrađivao osobne podatke posebne kategorije (zdravstvene podatke)** ispitanika u svojoj bazi (aplikaciji) **bez postojanja pravne osnove** iz članka 6. stavka 1. te s tim u vezi članka 9. stavka 2. Opće uredbe o zaštiti podataka.
4. Voditelj obrade **nije na transparentan i propisani način informirao ispitanike o obradi njihovih zdravstvenih podataka** u politikama privatnosti, a što je protivno članku 12. stavku 1. Opće uredbe o zaštiti podataka te s tim u vezi članku 13. stavku 1. i 2. Opće uredbe o zaštiti podataka.
5. **Za snimanje telefonskih razgovora** s ispitanicima u razdoblju od 25. svibnja 2018. godine do 16. siječnja 2019. godine, voditelj obrade **nije imao utvrđenu pravnu osnovu** iz članka 6. stavka 1. Opće uredbe o zaštiti podataka te je s tim u vezi došlo do povrede i članka 5. stavka 2. Opće uredbe o zaštiti podataka.
6. Voditelj obrade **nije na razumljiv i jasan način informirao ispitanike o obradi osobnih podataka u vidu snimanja telefonskih razgovora**, a čime je postupio protivno članku 12. stavku 1. Opće uredbe o zaštiti podataka.

Agenciji za naplatu potraživanja izrečena upravna novčana kazna u iznosu od 2,26 milijuna eura

Agencija za zaštitu osobnih podataka izrekla je upravnu novčanu kaznu voditelju obrade – agenciji za naplatu potraživanja B2 Kapital d.o.o. u iznosu od 2.265.000,00 eura (17.065.642,50 kuna) zbog sljedeće utvrđenih povreda Opće uredbe o zaštiti podataka:

1. **Voditelj obrade nije na jasan i točan način informirao svoje ispitanike o obradi njihovih osobnih podataka putem obavijesti o obradi osobnih podataka (politike privatnosti)**, a u pogledu pravne osnove kod povrata preplaćenih sredstava, što je protivno odredbi članka 13. stavka 1. Opće uredbe o zaštiti podataka. Time je došlo do netransparentne obrade osobnih podataka ispitanika (odnosno pogrešnog informiranja u pogledu pravne osnove obrade iz članka 6. stavka 1. Opće uredbe o zaštiti podataka) kojih je u trenutku provođenja nadzora bilo (najmanje) 132 652, a politika privatnosti ostala je nepromijenjena te povreda još nije otklonjena, odnosno traje od 25. svibnja 2018. do danas.

2. Protivno odredbi članka 28. stavka 3. Opće uredbe o zaštiti podataka, **voditelj obrade nije sklopio ugovor o obradi osobnih podataka s izvršiteljem obrade za uslugu praćenja jednostavnog stečaja potrošača** te je time ugrožena sigurnost osobnih podataka 83 896 ispitanika (OIB), budući da je sklapanje ugovora s izvršiteljem obrade jedna od svojevrsnih sigurnosnih poluga koja osigurava da su jasno ugovorena pravila obrade osobnih podataka, njihov tijek u poslovnom odnosu između voditelja i izvršitelja obrade te kako bi se voditelj obrade osigurao da izvršitelj obrade zadovoljava tehničke i organizacijske mjere zaštite kod obrade osobnih podataka velikog broja ispitanika. Utvrđeno je kako je navedena povreda trajala od prihvata ponude za pružanje usluge praćenja jednostavnog stečaja potrošača, odnosno od 14. veljače 2019. do 26. veljače 2021. kada je došlo do prekida poslovne suradnje.

NAJVEĆI PROBOJ DOSAD

Procurili podaci više milijuna hrvatskih vozača, doznajemo koja bi organizacija potencijalno mogla biti krivac

Među njima su, navodno, i podaci ministara, štićenih osoba i ambasadora. Oglasila se i SOA

> Procurili su podaci o registracijama, vozilima i više milijuna njihovih vlasnika, za Jutarnji je to potvrdilo više službi, uključujući i SOA-u.
>
> Nakon što je vijest prvo objavio Večernji list, navodeći da je riječ o 2,444.587 zapisa o vozilima, i to 1,195.052 fizičke osobe, koji su procurili iz baze podataka neke domaće institucije, sve su službe najavile istragu.
>
> Međutim, ono što iznenađuje jest da se još ne može utvrditi iz koje su institucije ili organizacije svi ti podaci iscurili. MUP i Centar za vozila Hrvatske, dvije službe koje imaju pristup navedenim podacima, prebacuju odgovornost, a AZOP, koji određuje visoke kazne za ovakve propuste, tek najavljuje istragu slučaju.

Podaci, navodno, sadrže imena vlasnika vozila, adrese, osobne identifikacijske brojeve, jedinstvene matične brojeve građana, datume rođenja, registracije i ostale podatke o policama osiguranja. Među njima su, navodno, i podaci ministara, štićenih osoba i ambasadora.

Da nije riječ o kibernetičkom napadu, nego o neovlaštenom kopiranju podataka od osoba koje su imale pristup informacijskom sustavu, potvrdili su za Jutarnji iz SOA-e. Sigurnosno-obavještajna agencija dobila je, naime, prijavu s USB-om.