General Data Protection Regulation

GDPR

Platforma

GDPR Platforma (General Data Protection Regulation Platform) formirana je sukladno europskoj Općoj uredbi o zaštiti podataka (EU 2016 / 679 Europskog parlamenta i Vijeća)

INFODOM

Opća uredba o zaštiti podataka usvojena je 27. travnja 2016., a primjenjuje se od 25. svibnja 2018.

Motivacija

Opća uredba o zaštiti podataka (GDPR) i zaštita privatnosti u korištenju osobnih podataka donesena je u uvjetima sveopće digitalizacije kroz koju se ostvaruju velike, nove prilike za poboljšanje poslovanja, ali istovremeno nastaju i nove opasnosti.

Uređenost u svijetu digitalizacije osigurava se kroz upravljanje digitalnim kanalima i osiguranje pravne interoperabilnosti za elektroničke dokumente i digitalizirane procese uz primjenu visoke razine tehnika kibernetske sigurnosti.

Zaštita privatnosti u korištenju osobnih podataka potpuno je odvojena od tehnologije na kojoj se prikupljaju, obrađuju, pohranjuju i distribuiraju podaci i dokumenti (neovisno da li su na papiru ili je sve digitalizirano).

Digitalizacija je proširila i pojačala zahtjeve i izvan dosadašnjeg Zakona o zaštiti osobnih podataka kroz nove oblike prava pojedinca (obveza privole, pravo na zaborav…).

Koje su obveze Službenika za zaštitu osobnih podataka?

Gartner™ u svom izvješću s kraja 2016. godine donosi zaključke istraživanja stanja usklađenosti europskih pa i globalnih tvrtki kroz pet visoko prioritetnih promjena koje svaka organizacija treba izvršiti kako bi se uskladila s GDPR uredbom. Na drugom mjestu Gartner™ preporuča: „Odmah osigurajte službenika za zaštitu osobnih podataka (DPO) čak i ako niste sigurni da li ste na to obavezni po Uredbi i osigurajte platformu unutar svoje organizacije za DPO kako bi bez prepreka omogućili suradnju sa stručnjacima za sigurnost te objedinili aktivnosti na podizanju svjesnosti i arhitekture privatnosti.

Službenik za zaštitu osobnih podataka (DPO - Data Protection Officer) uz našu će pomoć:

Kontinuirano pratiti usklađenost sa Uredbom:

- prikupljati informacije o aktivnostima obrada
- analizirati i provjeravati pravnu usklađenost obrada te
- informirati, savjetovati i davati preporuke voditelju i izvršitelju obrada

Procjenjivati učinke zaštite osobnih podataka pružanjem savjeta:

- je li potrebno provoditi analizu utjecaja na privatnost - DPIA (*Data Protection Impact Assessment*)
- koju metodologiju primijeniti u provedbi DPIA
- koje sigurnosne kontrole (procesne, tehničke i organizacijske) treba uspostaviti za umanjivanje rizika od povrede prava i interesa ispitanika

Sustavno će pristupati aktivnostima zaštite osobnih podataka temeljenih na rizicima:

- identificirati i ocjenjivati rizike te prioritizirati aktivnosti temeljem izloženosti riziku
- identificirati područja na kojima je potrebno provesti prioritetne provjere sigurnosti
- dati preporuke za edukaciju radnika odgovornih za obradu osobnih podataka te
- identificirati obrade na čiju je zaštitu potrebno obratiti dodatnu pažnju

Opća uredba o zaštiti podataka (GDPR – General Data Protection Regulation) unosi velike promjene u načine upravljanja osobnim podacima i izravno se primjenjuje na sve organizacije koje raspolažu osobnim podacima EU građana.

Prava pojedinca

Privola

Prema Uredbi, svaka pravna ili fizička osoba koja na bilo koji način prikuplja osobne podatke o pojedincu za daljnju obradu bez zakonske osnove trebat će izričitu privolu (Consent) pojedinca. Prilikom traženja privole, pojedincu na jasan i jednostavan način treba biti izrečeno koji se podaci pohranjuju, u koju svrhu i, ukoliko je moguće, na koje razdoblje.

Pravo na zaborav

Pojedinac ima pravo zatražiti brisanje osobnih podataka (*Right to be Forgotten*) kako bi spriječio njihovu daljnju obradu. To znači povlačenje prvotno dane privole ili prestanak temelja za korištenje podataka. No, ukoliko neki drugi zakon nalaže čuvanje osobnih podataka (npr. zbog ugovorne obveze 2 godine) tada se podaci ne mogu brisati na zahtjev pojedinca sve dok ne istekne zakonom zadan rok čuvanja.

Pravo na pristup

U bilo kojem trenutku pojedinac će moći zatražiti pristup (*Right to Access*) svojim osobnim podacima koje fizička ili pravna osoba obrađuje te zatražiti informaciju o tome gdje i za koju svrhu se oni koriste. Ovim pravom se postiže transparentnost podataka, čime se dobiva povjerenje samog pojedinca.

Pravo na prenosivost

Pojedinac dobiva pravo na prijenos (*Data Portability*) osobnih podataka te može zatražiti da pravna ili fizička osoba koja trenutno obrađuje njegove podatke te iste podatke pošalje u sigurnom obliku i sigurnim putem trećoj strani i to samo u slučaju automatske obrade temeljem ugovora ili privole.

Povreda osobnih podataka

Ukoliko dođe do curenja osobnih podataka, napada ili nedopuštenog korištenja osobnih podataka, pravna ili fizička osoba u roku od 72 sata mora obavijestiti nadležno nadzorno tijelo, ali i samog pojedinca.

Što moraju učiniti obveznici primjene Uredbe?

Obveznici imaju zadatak pružiti pojedincima sva prava propisana Uredbom te dizajnirati svoje poslovne procese i informacijske sustave kako bi se na najbolji mogući način sačuvao identitet pojedinca od bilo kakvog curenja podataka, napada itd. ugradnjom *Privacy by Design* principa u organizaciju.

Svaki obveznik mora imenovati osobu koja će se brinuti jesu li odredbe Uredbe implementirane na ispravan način, koja će savjetovati menadžment i zaposlenike, obučavati i podizati razinu svijesti o zaštiti podataka, provoditi nadzor te surađivati s nadzornim tijelima.

Uredba takvu osobu naziva Službenik za zaštitu osobnih podataka (DPO - *Data Protection Officer*) te nalaže da mora imati profesionalne kvalitete i stručno znanje na području prakse i propisa o zaštiti podataka.

Podaci koji se prikupljaju za daljnju obradu moraju biti obrađeni u skladu sa zakonom, na pošten i transparentan način u odnosu prema pojedincu.

Količina podataka koja se prikuplja mora biti minimizirana, što znači da se ne smiju prikupljati nepotrebni podaci i koristiti u druge svrhe.

Striktno se određuje koji se podaci koriste za koju svrhu i to je eksplicitno navedeno u privoli koju pojedinac daje. Također, podaci moraju biti ažurni, a pojedinac ima pravo ispravljati i mijenjati prikupljene podatke.

Obveznik mora definirati:

- ✓ što su sve osjetljivi podaci u njihovim sustavima,
- ✓ gdje se sve nalaze takvi podaci,
- ✓ tko sve ima pristup takvim podacima,
- ✓ kako se podaci kreću kroz sustav i koliki je rizik,
- ✓ kako su podaci zaštićeni,
- ✓ plan na koji način će se provoditi Uredba.

Prije implementacije bilo kakvih organizacijskih, proceduralnih i tehnoloških rješenja, potrebno je napraviti inicijalnu analizu utjecaja na privatnost (*Data Protection Impact Assessment*) i snimku stanja kako bi se ustanovile neusklađenosti te izraditi program usklađivanja.

Poslovni zahtjevi

Digitalni kanali i umreženost

Upravljanje digitalnim kanalima i prometom digitalnih sadržaja, u elektroničkim dokumentima i transakcijama, inicijalni je problem digitalne transformacije.

Integrirano upravljanje kontaktima s okolinom i generiranje konkurentske prednosti iz takvog pristupa, ključno je pitanje poslovanja, jer se sve više kontakata sa kupcima, dobavljačima i poslovnom okolinom obavlja digitalno. Gotovo svi ljudi danas imaju mobilne uređaje sa sobom i mogu ih koristiti kao fizičke osobe, ali i kao zaposlenici. Svojim kontaktima i vlastitim osobnim podacima i korištenjem ostavljaju digitalne tragove na serverima.

Jedinstvena točka pristupa

Sve institucije i poduzeća danas imaju portale radi prisutnosti na Internetu, ali i razmjenu elektroničkih poruka i dokumenata između njihovih informacijskih sustava. Na društvenim mrežama (Facebook, Twitter, LinkedIn, YouTube…) razmjenjuju se svi oblici sadržaja i osobnih podataka tako da je za obveznike kritično zaštititi osobne podatke.

Pristup digitalnim kanalima omogućava kontakte i komunikaciju prema svim dionicima u ekosustavu poduzeća:

- kupci, dobavljači i principali,
- država i poslovna okolina,
- znanstveno-istraživačka zajednica,
- mediji,
- menadžeri i radnici.

Kako Vam InfoDom može pomoći?

Glavne primjene GDPR platforme

Digitalna interakcija poslovnog subjekta s okolinom mora omogućiti razmjenu i primjerenu zaštitu različitih osobnih podataka, elektroničkih dokumenata i digitalnih isporuka koje sadrže osobne podatke, a vezani su za infrastrukturne informacijske sustave (RMS, CMS, KMS, DA, CRM, ERP, SCM, HCM, DWH…):

- eZahtjevi, eNarudžbe, eIsporuke, eRačuni, ePlatni Nalozi
- Kontrolne liste, Ankete, Upitnici, Newsletter-i
- Upiti kupaca, Reklamacije
- Dokumenti s osobnim podacima prema poreznim i drugim tijelima državne uprave te dobavljačima usluga
- Dokumenti prema regulatorima
- Radno-pravni dokumenti prema menadžerima i radnicima.

GDPR platforma omogućava sveobuhvatnu digitalizaciju i zaštitu osobnih podataka, upravljanje rizicima te omogućava agilne promjene ponašanja poslovnog subjekta (novi poslovni modeli, inovacije proizvoda, inovacije procesa...) uz ugradnju principa *Privacy by Design* u organizaciju. Najvažniji je učinak higijena na digitalnim kanalima komunikacije.

Transparentnost podataka

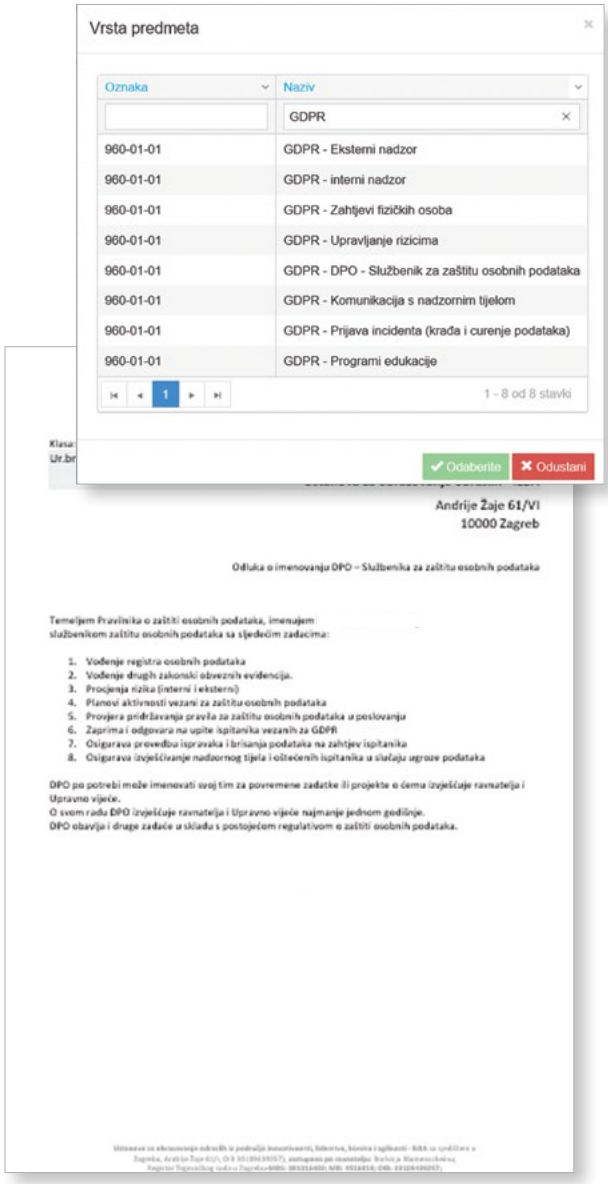
Svaki obveznik raspolaže s većom količinom podataka nego je potrebno za poslovanje. Ali, nema dovoljno ili uopće nema informacija o svim njihovim lokacijama pohrane, njihovoj strukturi, njihovoj upotrebi i zaštiti sukladno zahtjevima Uredbe.

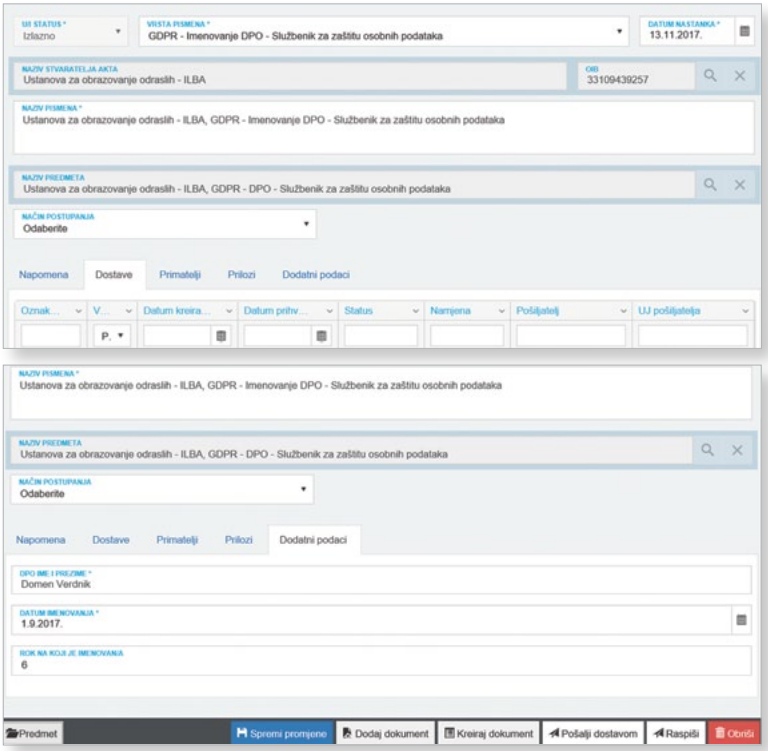
GDPR platforma daje rješenja sukladno zahtjevima Uredbe koja omogućavaju zaštitu podataka te uspostavu i vođenje evidencija o obradi osobnih podataka i procesima u kojima se ta obrada odvija. To omogućava zadovoljenje zahtjeva nadzornog tijela, kupaca, korisnika i radnika te brzu i učinkovitu reakciju u slučaju povrede osobnih podataka.

Upravljanje poslovnim procesima GDPR sustava

Ključni procesi prema Uredbi:

1. Governance GDPR i interne politike
2. Upravljanje usklađenosti (*Compliance*)
3. Ishođenje privola i zahtjeva za realizaciju prava na zaštitu podataka
4. Realizacija prava na brisanje podataka
5. Upravljanje povredama osobnih podataka
6. Upravljanje korektivnim mjerama
7. Vođenje evidencija obrade (registara i kataloga)
8. Upravljanje rizicima
9. Upravljanje rizicima treće strane
10. Praćenje vanjskih događaja
11. Potporni poslovi za GDPR sustav





Operativni postupci za kontrolu zaštite osobnih podataka pomoću kontrolnih listi:

- Evaluacija procesa prema zahtjevima Uredbe
- Definiranje na kojim koracima procesa će se raditi kontrola zaštite osobnih podataka
- Bilježenje svih događaja unutar nekog procesa
- Automatska validacija odgovora kontrolne liste
- Automatsko slanje upozorenja i prijedloga za akcije
- Definiranje alarma
- Izvješćivanje
- Najbolje prakse (*Best Practices*) zaštite osobnih podataka i naučene lekcije (*Lessons Learned*)

Upravljanje rizicima

U uvjetima digitalizacije zaštita osobnih podataka i sigurnost zahtijevaju veću pozornost obveznika Uredbe te ih upućuje na procjenu utjecaja na privatnost prilikom uvođenja novih tehnologija.

Upravljanje vanjskim i internim rizicima, eksternim i internim događajima omogućava povećanje sposobnosti brže reakcije na povredu osobnih podataka te konzistentnu provedbu reakcije, ali i rješavanje problema iz incidenata te razvijanje preventivno – korektivnih mjera i fokusirano djelovanje temeljeno na procjenama rizika.

Kroz takve sposobnosti, koje uključuju i adaptabilnost na nepoznate događaje, obveznici bitno povećavaju svoju organizacijsku svjesnost o odnosu s okolinom i vlastitim ekosustavom pa time i povećavaju usklađenost sa zahtjevima Uredbe.

Komercijalizaciju novih sposobnosti obveznici postižu smanjenjem šteta od incidenata, ali još važnije, pravovremenim reakcijama na poslovne prilike, izvršavanje zakonskih obveza i ostvarenje novih prihoda.

Podrška menadžmenta

Čak i najmanji pogrešni korak u postupanju s osobnim podacima može rezultirati nepridržavanjem zahtjeva Uredbe. Potrebno je osigurati da svi radnici razumiju osnovne zahtjeve Uredbe i vlastitu ulogu u zaštiti osobnih podataka posebno zbog visokih kazni i reputacijskog rizika.

GDPR platforma osigurava provođenje zahtjeva i načela Uredbe za usklađenost standardiziranim postupcima, dokumentima, najboljim praksama zaštite osobnih podataka i e-Learning sadržajima u cilju kontinuiranog osvješćivanja radnika u području zaštite osobnih podataka te na koji način postupiti u slučaju povrede osobnih podataka.

Izvješćivanje

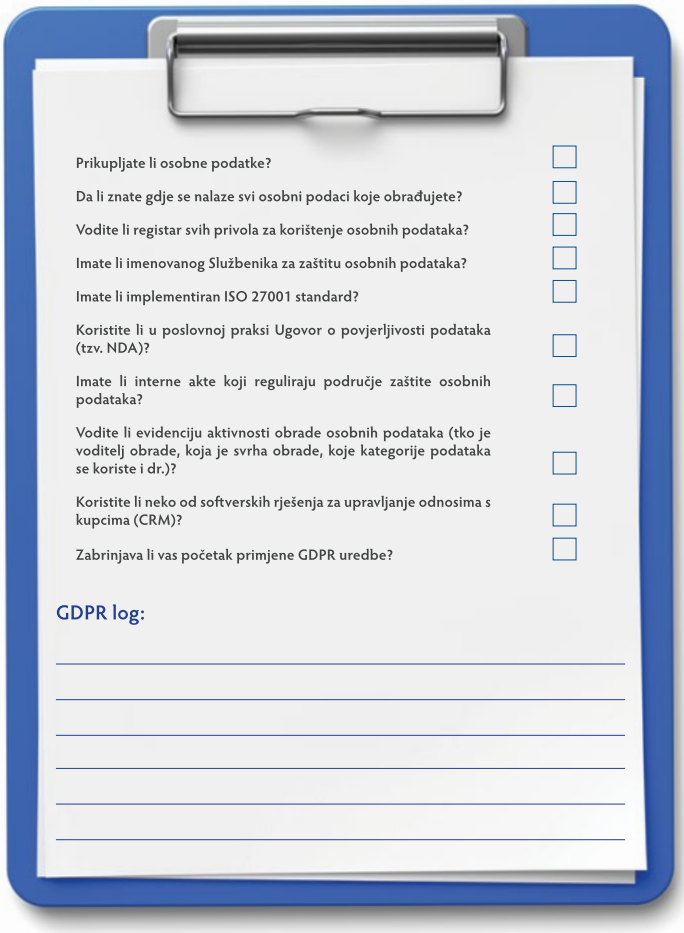
Komunikacija postaje strateško i taktičko sredstvo protiv povrede osobnih podataka. Obveznici bi trebali osigurati interese unutarnjih i vanjskih subjekata za dobivanjem informacija o obradi i o povredi osobnih podataka.

Izvještajni sustav GDPR platforme omogućava izvješćivanje o statusu usklađenosti te o dokazima o zakonitoj obradi osobnih podataka.

Efekti primjene **GDPR** platforme

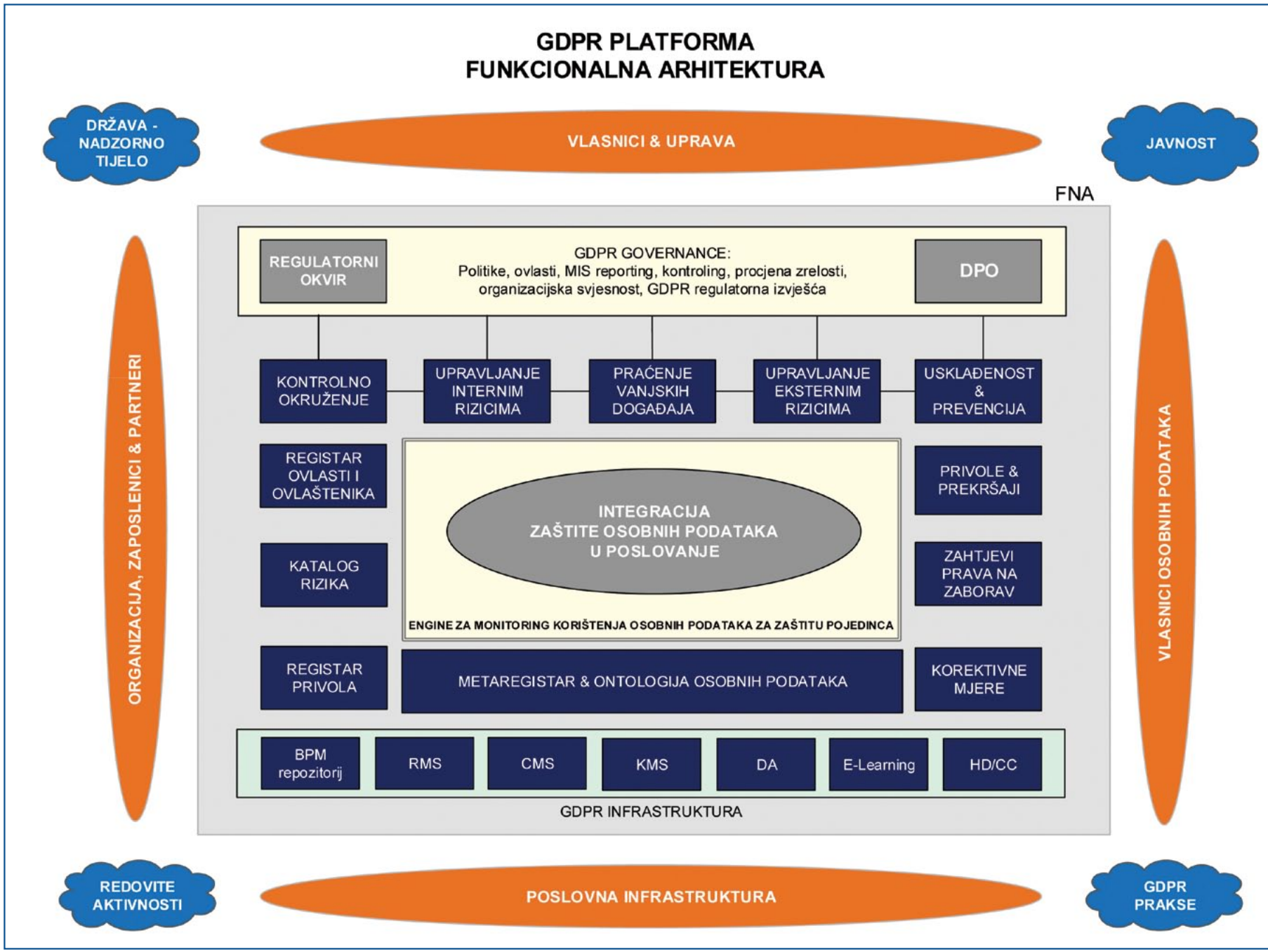
Implementacijom GDPR platforme, kroz integrirano upravljanje digitalnim kanalima i interakcijom prema svim subjektima, postižu se efekti za obveznike i osobe u visokoj zaštiti osobnih podataka:

- Kontinuirani monitoring korištenja osobnih podataka za zaštitu pojedinca
- Vođenje Registra osobnih podataka
- Vođenje Kataloga rizika
- Vođenje Registra ovlasti i ovlaštenika
- Vođenje Registra privola
- Upravljanje rizicima vezanim uz prikupljanje i obradu osobnih podataka - Sustavno, ponovljivo, transparentno i svrsishodno - DPIA (*Data Protection Impact Assessment*) kao preduvjet za *Privacy by Design* princip
- Upravljanje privolama, zahtjevima prava na zaborav, prigovorima, incidentima, prekršajima
- Standardizirani poslovni procesi u zaštiti osobnih podataka
- Standardizirani predlošci dokumenata
- Kontroling korektivnih mjera za zaštitu osobnih podataka
- Praćenje povijesnosti događaja („Audit trag" upotrebe osobnih podataka) - kontrolabilnost i korištenje u pravnim pitanjima u poslovanju s okolinom, ali i za potrebe poslovnog kontinuiteta
- Alarmi na približavanje isteka zakonskog roka za odgovor na zahtjeve u vezi obrade osobnih podataka, na istek zakonskog roka za čuvanje osobnih podatka
- Standardizirana izvješća prema:
  - nadzornom tijelu
  - vlasniku osobnih podataka u vezi provedenih promjena na njegovim podacima
  - vlasniku / upravi



Ovo je samo Vaša inicijalna GDPR kontrolna lista.

U okviru GDPR Platforme postoji niz kontrolnih listi za različite faze, aktivnosti i poslovne situacije.

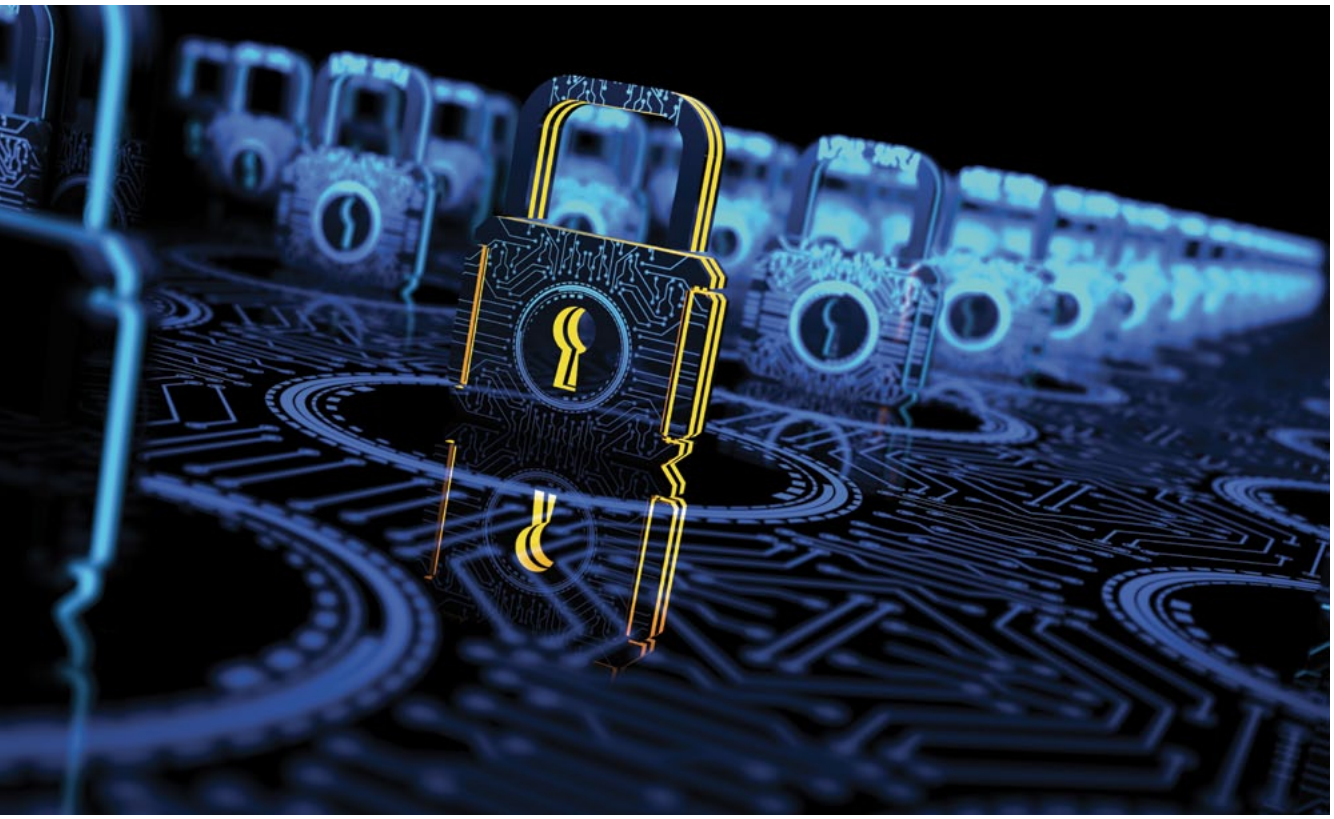

GDPR PLATFORMA
FUNKCIONALNA ARHITEKTURA
DRŽAVA - NADZORNO TIJELO
VLASNICI & UPRAVA
JAVNOST
FNA
ORGANIZACIJA, ZAPOSLENICI & PARTNERI
REGULATORNI OKVIR
GDPR GOVERNANCE:
Politike, ovlasti, MIS reporting, kontroling, procjena zrelosti, organizacijska svjesnost, GDPR regulatorna izvješća
DPO
KONTROLNO OKRUŽENJE
UPRAVLJANJE INTERNIM RIZICIMA
PRAĆENJE VANJSKIH DOGAĐAJA
UPRAVLJANJE EKSTERNIM RIZICIMA
USKLAĐENOST & PREVENCIJA
REGISTAR OVLASTI I OVLAŠTENIKA
PRIVOLE & PREKRŠAJI
INTEGRACIJA ZAŠTITE OSOBNIH PODATAKA U POSLOVANJE
KATALOG RIZIKA
ZAHTJEVI PRAVA NA ZABORAV
ENGINE ZA MONITORING KORIŠTENJA OSOBNIH PODATAKA ZA ZAŠTITU POJEDINCA
REGISTAR PRIVOLA
METAREGISTAR & ONTOLOGIJA OSOBNIH PODATAKA
KOREKTIVNE MJERE
BPM repozitorij
RMS
CMS
KMS
DA
E-Learning
HD/CC
GDPR INFRASTRUKTURA
VLASNICI OSOBNIH PODATAKA
REDOVITE AKTIVNOSTI
POSLOVNA INFRASTRUKTURA
GDPR PRAKSE

Saznajte zašto je GDPR Platforma Vaš pravi izbor za regulatornu usklađenost i digitalnu interakciju s okolinom.

Kontaktirajte nas!

InfoDom d.o.o.
t: + 385 1 3040 588
e: infodom@infodom.hr

goo.gl/U7E7Zg



INFODOM

InfoDom d.o.o.
Andrije Žaje 61/I
10000 Zagreb - Hrvatska
t: + 385 1 3040 588
f: + 385 1 3040 593
e: infodom@infodom.hr

InfoDom Sarajevo d.o.o. / Fra Anđela Zvizdovića 1 / 71000 Sarajevo, Bosna i Hercegovina / e: info@infodom.ba
InfoDom CG d.o.o. / Ul. Dž. Vašingtona 3/19 / 81000 Podgorica, Crna Gora / e: info@infodom.me
InfoDom SEE d.o.o. / V. Popovića 38-40 / 11070 Beograd, Srbija / e: info@infodom.rs
InfoDom WE LTD / 88 Wood Street / EC2V 7RS London, United Kingdom

QUALITY SYSTEM CERTIFICATION DNV·GL ISO 9001

ISO 20000 BUREAU VERITAS Certification

ISO 27001 BUREAU VERITAS Certification