

## POLITIKA SUSTAVA UPRAVLJANJA OSOBNIM PODACIMA

### Sadržaj

1. PREDMET .....	2
2. REFERENTNI DOKUMENTI .....	2
3. PRIKUPLJANJE I OBRADA .....	2
4. PRAVA ISPITANIKA.....	2
5. EVIDENCIJA OBRADA OSOBNIH PODATAKA .....	3
6. ZAŠTITA PODATAKA.....	3
7. UPRAVLJANJE INCIDENTIMA .....	3
8. CERTIFIKACIJA.....	4
9. IZNIMKE .....	4
10. ODGOVORNOST.....	4
11. VALJANOST I UPRAVLJANJE DOKUMENTOM.....	5

## 1. Predmet

Ovom Politikom Uprava Gemma B&D d.o.o. daje punu podršku sustavu upravljanja osobnim podacima. Sustav upravljanja osobnim podacima potrebno je u potpunosti uskladiti s Uredbom (EU) 2016/679 o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka. Svrha zaštite osobnih podataka je zaštita privatnog života i ostalih ljudskih prava i temeljnih sloboda u prikupljanju, obradi i korištenju osobnih podataka. Osobni podatak je svaka informacija koja se odnosi na fizičku osobu koja je identificirana ili se može identificirati. Ovim se podacima mora pristupiti posebnom pažnjom, te se pri tome mora voditi najvišim etičkim načelima. Nužno je raditi na podizanju svijesti da su osobni podaci vrlo vrijedna i povjerljiva imovina. Potrebno je razviti i provoditi program izgradnje korporativne kulture čuvanja povjerljivosti osobnih podataka.

## 2. Referentni dokumenti

- Uredba (EU) 2016/679

## 3. Prikupljanje i obrada

Prikupljanje i obrada osobnih podataka dozvoljeni su isključivo kada postoji zakonska obveza ili obveza temeljena na ugovornom odnosu, dok su sve ostale obrade osobnih podataka dozvoljene uz jasnu privolu vlasnika ili njihovih opunomoćenika. Podaci moraju biti točni i potpuni i razmjerni svrsi u koju se obrađuju. Prilikom prikupljanja osobnih podataka ispitaniku se mora pružiti informacija o svojem identitetu i kontakt podacima, svrhama obrade i pravnoj osnovi za obradu podataka, primateljima, iznošenju u treće zemlje, razdoblju pohrane, mogućnosti povlačenja privole. Prikupljanju osobnih podataka od djece mora se pristupiti sa posebnom pažnjom, te se pri tome mora voditi najvišim etičkim načelima.

## 4. Prava ispitanika

- Ispitaniku je potrebno pružiti sve informacije u vezi s obradom, u sažetom, transparentnom, razumljivom i lako dostupnom obliku.
- Ispitanik ima pravo uvida u osobne podatke, koji se nalaze u zbirkama podataka i koji se na njega odnose.
- Ispitanik ima pravo ishoditi ispravak netočnih osobnih podataka, koji se na njega odnose.

- Ispitanik ima pravo ishoditi brisanje osobnih podataka, koji se na njega odnose i za koje je dao privolu.
- Ispitanik ima pravo na odustajanje od dane privole za obradu osobnih podataka i traženje prestanka obrade osobnih podataka.
- Ispitanik ima pravo zaprimiti osobne podatke, koji se odnose na njega, a koje je pružio voditelju obrade u strukturiranom, uobičajeno upotrebljavanom i strojno čitljivom formatu.

## 5. Evidencija obrada osobnih podataka

Gemma B&D d.o.o. će uspostaviti centralnu evidenciju svih zbirki osobnih podataka. Za svaku zbirku potrebno je imenovati odgovornu osobu. Zbirka obrade mora sadržavati identitet voditelja s kontakt podacima, svrhu obrade, opis ispitanika i osobnih podataka, primatelje podataka, informacije o prijenosu podataka u treće zemlje, predviđene rokove čuvanja podataka.

## 6. Zaštita podataka

Gemma B&D d.o.o. će poduzeti sve potrebne tehničke, administrativne i fizičke mjere zaštite osobnih podataka kako bi se podaci zaštitili od neovlaštenih pristupa i moguće zlouporabe. Kod izgradnje novih informacijskih sustava, od samog početka, mora se uzeti u obzir zahtjeve GDPR-a za zaštitu osobnih podataka i osigurati njihovu provedbu.

## 7. Upravljanje incidentima

Potrebno je uspostaviti i održavati:

- plan odgovora na incidente vezane za narušavanje sigurnosti osobnih podataka.
- registar incidenata narušavanja sigurnosti osobnih podataka.
- proces za obavještanje nadzornog tijela i oštećene osobe o incidentima narušavanja sigurnosti osobnih podataka.

U slučaju narušavanja sigurnosti osobnih podataka potrebno je bez odlaganja, a najkasnije u roku od 72 sata po otkrivanju incidenta, o tome izvijestiti nadležno tijelo. U slučaju curenja osobnih podataka potrebno je obavijestiti i vlasnike, čiji su podaci kompromitirani, o povredi osobnih podataka koristeći se jasnim i jednostavnim jezikom.

## 8. Certifikacija

Svoj sustav upravljanja osobnim podacima, Gemma B&D d.o.o. će uspostaviti i održavati sukladno primjenjivim standardima iz područja zaštite privatnosti i informacijske sigurnosti ISO 27001, a usklađenost će dokazivati odgovarajućom certifikacijom kada je to moguće.

## 9. Iznimke

Ako postoje opravdani razlozi, Službenik za zaštitu osobnih podataka može odobriti privremeno postupanje s osobnim informacijama, koje nije u skladu s ovom Politikom. Službenik za zaštitu osobnih podataka dužan je voditi evidenciju ovakvih odobrenja, odgovornosti i rokova za usklađivanje, te o tome izvještavati Upravu.

## 10. Odgovornosti

- Svi zaposlenici moraju se pridržavati mjera definiranih ovom Politikom, kao i treće strane, koje u okviru svoje suradnje s Gemma B&D d.o.o. ostvaruju pristup osobnim podacima.
- Službenika za zaštitu osobnih podataka imenuje Uprava i on je za rad odgovoran direktno Upravi. Za uspostavu i održavanje sustava upravljanja osobnim podacima, te koordinaciju svih aktivnosti vezanih uz upravljanje osobnim podacima, odgovoran je Službenik za zaštitu osobnih podataka. Službenik za zaštitu osobnih podataka odgovoran je za:
  - obavještanje i savjetovanje voditelja ili izvršitelja obrade, te zaposlenika koji obrađuju osobne podatke o njihovim obavezama iz Uredbe,
  - nadziranje poštivanja Uredbe i internih politika i ostale regulative, vezane uz zaštitu osobnih podataka,
  - uspostavu i održavanje registra osobnih podataka,
  - dodjela odgovornosti za zaštitu osobnih podataka zaposlenicima i trećim stranama, uključenima u prikupljanje i obradu osobnih podataka,
  - podizanje svijesti i edukacija iz područja zaštite osobnih podataka,
  - ugrađivanje zaštite privatnosti u poslovne procese i informacijske sustave,
  - ugrađivanje zaštite privatnosti u revizijske procese,
  - savjetovanje kod provedbi procjena učinka na zaštitu podataka,
  - suradnja s nadzornim tijelima,
  - nadziranje procesa upravljanja rizikom, u obradama osobnih podataka

- o izvještavanje Uprave o učinkovitosti sustava upravljanja osobnim informacijama

Ova se Politika revidira najmanje jednom godišnje ili nakon svake izmjene u pravnom okruženju ili okruženju rizika koja bi mogla imati učinak na njenu učinkovitost. Za održavanje ove Politike zadužen je Službenik za zaštitu osobnih podataka.

## 11. Valjanost i upravljanje dokumentom

Ovaj dokument stupa na snagu nakon odobrenja Uprave u obliku vlastoručnog potpisa.

Vlasnik ovog dokumenta je Uprava, koja ga je dužna najmanje jednom godišnje revidirati, te po potrebi preinačiti. Ovaj dokument potrebno je izmijeniti, ako se značajno promijeni broj ili struktura zaposlenih, ili ako Gemma B&D d.o.o. promijeni politiku poslovanja.

	Datum	Ime i prezime	Funkcija	Potpis
Izradio/la:	25.05.2018.	Koraljka Soušek	Direktorica FiR	
Odobrio/la:	30.05.2018	Davor Jurčić	Direktor Društva	