

Pravilnik o zaštiti osobnih podataka

eBurza Grupa d.o.o. • Green Tech i Svijet Beba poslovni sustavi

Voditelj obrade	eBurza Grupa d.o.o.
Verzija	1.0 / 28. kolovoza 2026.
Kontakt za zaštitu podataka	Zvonimir Lisec • gdpr@green-tech.hr
Status dokumenta	Interni akt - za primjenu u poslovanju društva

Dokument se preispituje najmanje jednom godišnje te bez odgađanja nakon značajne promjene procesa obrade, informacijskih sustava, propisa ili organizacije.

1. Predmet i svrha Pravilnika

Ovim Pravilnikom eBurza Grupa d.o.o. uređuje organizacijska i tehnička pravila zaštite osobnih podataka u svim poslovnim procesima društva, uključujući internetske trgovine Green Tech i Svijet Beba, maloprodaju, skladište, marketing, upravu, rad sa zaposlenicima i studentima te suradnju s vanjskim pružateljima usluga.

Cilj je osigurati zakonitu, poštenu, transparentnu i sigurnu obradu osobnih podataka, uz primjenu načela smanjenja količine podataka, ograničenja svrhe, točnosti, ograničenja pohrane, cjelovitosti i povjerljivosti te dokazivosti usklađenosti.

2. Pravni okvir

- Uredba (EU) 2016/679 (Opća uredba o zaštiti podataka - GDPR), osobito članci 5., 6., 12.-22., 24.-32., 33.-35. i 37.-39.
- Zakon o provedbi Opće uredbe o zaštiti podataka (NN 42/18), uključujući odredbe o videonadzoru.
- Zakon o računovodstvu i porezni propisi u dijelu obveznog čuvanja poslovne i računovodstvene dokumentacije.
- Zakon o zaštiti potrošača u dijelu prigovora, reklamacija, ugovora na daljinu i dokazivanja komunikacije s potrošačem.
- Zakon o radu i drugi posebni propisi koji uređuju podatke zaposlenika, studenata i kandidata za posao.
- Drugi primjenjivi hrvatski i europski propisi o elektroničkim komunikacijama, informacijskoj sigurnosti i poslovnoj dokumentaciji.

3. Voditelj obrade i organizacija

Voditelj obrade	eBurza Grupa d.o.o.
Adresa	Kralji 13, 10360 Sesvete, Republika Hrvatska
OIB	32564605678
Poslovni sustavi / kanali	Green Tech i Svijet Beba
Kontakt	info@green-tech.hr
Kontakt za zaštitu podataka	Zvonimir Lisec, gdpr@green-tech.hr

Društvo trenutačno ne imenuje službenika za zaštitu podataka (DPO). Uprava najmanje jednom godišnje i kod značajne promjene poslovanja procjenjuje jesu li nastupile okolnosti zbog kojih bi imenovanje DPO-a postalo obvezno. Zvonimir Lisec obavlja internu koordinaciju pitanja zaštite podataka bez statusa formalno imenovanog DPO-a.

Organizacijske cjeline obuhvaćene ovim Pravilnikom su Uprava, prodaja, skladište i marketing. Računovodstvene poslove obavlja vanjski servis 3 LINIJE d.o.o. za usluge, Ulica Vladimira Nazora 5, 10360 Sesvete, OIB 21576035283. Studenti koji sudjeluju u pakiranju narudžbi nemaju pristup administraciji webshopa, ali su obvezni čuvati povjerljivost podataka koje mogu vidjeti na dostavnoj i radnoj dokumentaciji.

4. Kategorije ispitanika i osobnih podataka

- Kupci i korisnici webshopova: ime i prezime, adresa, e-mail, telefon, podaci o narudžbi, IP adresa i tehnički zapisi.
- Poslovni kupci: dodatno OIB, naziv tvrtke, adresa i podaci potrebni za R1/e-račun.
- Korisnici koji podnose reklamaciju, servisni zahtjev, povrat ili raskid ugovora: podaci zahtjeva, proizvoda, računa, komunikacije i dokumentacije.
- Zaposlenici i studenti: identifikacijski, kontaktni, radno-pravni, obračunski i organizacijski podaci potrebni za rad i ispunjenje zakonskih obveza.
- Kandidati za posao: podaci iz životopisa, prijave i komunikacije tijekom selekcije.
- Pretplatnici na newsletter: e-mail, evidencija privole i odjave.
- Posjetitelji web stranice: IP adresa, kolačići i analitički podaci kada postoji odgovarajući pravni temelj/privola.
- Osobe obuhvaćene videonadzorom u i neposredno uz poslovni prostor, u granicama dopuštenim propisima.

5. Pravne osnove obrade

Društvo prije svake obrade utvrđuje svrhu i pravnu osnovu. Najčešće pravne osnove su:

- izvršenje ugovora ili poduzimanje radnji na zahtjev ispitanika prije sklapanja ugovora - narudžbe, dostava, korisnička podrška i izvršenje ugovornih obveza;
- zakonska obveza - računi, porezne i računovodstvene evidencije, potrošački prigovori i druge propisane evidencije;
- legitimni interes - sigurnost sustava, sprječavanje zlouporabe, zaštita imovine i obrana pravnih zahtjeva, nakon procjene interesa i prava ispitanika;
- privola - newsletter, marketinške tehnologije/kolačići kada je privola potrebna te druge dobrovoljne aktivnosti;
- druge osnove predviđene GDPR-om ili posebnim propisima kada su primjenjive.

Važno - checkout i GDPR

Podaci nužni za izvršenje narudžbe ne obrađuju se na temelju privole kupca. Kupcu se daje jasna Politika privatnosti. Privola se traži samo kada je za pojedinu svrhu stvarno potrebna, primjerice za newsletter ili određene marketinške kolačiće.

6. Informacijski sustavi i lokacije obrade

- Green Tech webshop - PHP/MySQL.

- Svijet Beba webshop - PHP/MySQL.
- Hosting Fastserver / Info-Impero d.o.o.; produkcijski server i hosting usluge nalaze se u Republici Hrvatskoj.
- E-mail sustav - lokalna pohrana i cPanel; SMTP2GO se koristi za slanje transakcijskih i servisnih poruka.
- AProSS skladišno-poslovni sustav društva ZGDATA za račune, skladište i poslovne evidencije.
- Synology poslužitelj u poslovnom okruženju za internu pohranu i sigurnosne kopije; koristi se i Dropbox kao dodatni backup/cloud servis.
- Računala zaposlenika u poslovnom prostoru na Slavonskoj aveniji 65, 10360 Sesvete.
- Google Analytics, uz primjenu odgovarajućeg mehanizma privole i postavki zaštite privatnosti.
- Videonadzor poslovnog prostora - unutarnji prostor i neposredni ulaz/pristup, bez nedopuštenog zahvaćanja javnih ili tuđih površina.

7. Primatelji i vanjski pružatelji usluga

Osobni podaci dostavljaju se samo u opsegu potrebnom za konkretnu svrhu. Glavne kategorije primatelja i pružatelja usluga su:

Primatelj / sustav	Svrha	Napomena o ulozi
GLS	dostava i praćenje pošiljke	primatelj podataka za izvršenje dostave
CorvusPay	kartično plaćanje	specijalizirani pružatelj platnih usluga; Green Tech ne pohranjuje pune podatke kartice
3 LINIJE d.o.o.	vanjsko računovodstvo	obrađuje podatke potrebne za računovodstvene i zakonske obveze
ZGDATA / AProSS	skladišno-poslovni sustav i podrška	pristup se ograničava na potrebni opseg i ugovorene svrhe
Fastserver / Info-Impero d.o.o.	hosting, backup weba i e-maila	tehnička obrada prema ugovorenim uslugama
SMTP2GO	slanje e-mailova	prijenos podataka potreban za dostavu elektroničkih poruka; primjenjuju se ugovorne zaštitne mjere

Primatelj / sustav	Svrha	Napomena o ulozi
Google Analytics	web analitika	samo uz odgovarajući pravni temelj/privolu i postavke privatnosti
Dropbox	dodatna sigurnosna pohrana	pristup ograničen; međunarodni prijenosi, ako postoje, moraju imati odgovarajuće zaštitne mjere
A1 Hrvatska	telekomunikacijske usluge	samostalni pružatelj telekomunikacijskih usluga

Za pružatelje koji djeluju kao izvršitelji obrade društvo osigurava odgovarajući ugovorni odnos prema članku 28. GDPR-a. Prije uključivanja novog pružatelja procjenjuju se sigurnost, lokacija obrade i eventualni prijenosi podataka izvan EGP-a.

8. Rokovi čuvanja i brisanje

Kategorija / obrada	Rok	Napomena
Operativni webshop podaci neregistriranih kupaca	do 3 mjeseca nakon izvršenja narudžbe	nakon toga se brišu iz operativnog webshop sustava, osim podataka koje je potrebno zadržati po drugoj osnovi
Računi i knjigovodstvene isprave	najmanje 11 godina	u skladu sa Zakonom o računovodstvu i povezanim poreznim propisima
Pisani prigovori potrošača	najmanje 1 godina od primitka	dulje ako je potrebno zbog otvorenog spora, reklamacije ili pravnog zahtjeva
Reklamacije, servis, povrat i jamstvo	za trajanja postupka i potrebnog razdoblja za dokazivanje prava i obveza	rok se određuje prema jamstvu, ugovornom odnosu i primjenjivim rokovima zastare

Kategorija / obrada	Rok	Napomena
Office / digitalne suglasnosti	najmanje za vrijeme u kojem je potrebno dokazivati ugovor i izjavu kupca	minimalni zapis čuva se uz narudžbu i dokaz isporuke digitalnog sadržaja
Korisnički račun	do zatvaranja računa ili prestanka svrhe	zakonske evidencije povezane s računom čuvaju se zasebno prema propisanim rokovima
Newsletter privola	do povlačenja privole	minimalna evidencija privole/odjave može se čuvati radi dokazivanja usklađenosti i sprječavanja ponovnog slanja
Web / sigurnosni logovi i IP adrese	do 3 mjeseca, osim sigurnosnog incidenta	dulje samo ako je potrebno za istragu incidenta ili pravni zahtjev
Kandidati za posao	do 6 mjeseci nakon završetka natječaja	dulje samo uz zasebnu privolu ili drugu zakonitu osnovu
Zaposlenici i studenti	za trajanja odnosa i nakon toga prema radnim, poreznim i drugim propisima	rokovi ovise o vrsti evidencije
Videonadzor	7 dana	izdvojena snimka može se čuvati dulje ako je dokaz u odgovarajućem postupku ili incidentu
Sigurnosne kopije	prema dokumentiranoj backup rotaciji	brisani podaci mogu privremeno ostati u backupu do prepisivanja; backup se ne koristi kao aktivna baza podataka

9. Upravljanje pristupima i povjerljivost

- Pristup osobnim podacima daje se prema načelu najmanjih potrebnih ovlasti i stvarnim radnim zadacima.
- Zaposlenici koriste individualne korisničke profile na računalima; uređaji se zaključavaju PIN-om ili drugim odgovarajućim mehanizmom.

- Windows Defender koristi se kao osnovna antimalware zaštita; sigurnosne nadogradnje operacijskog sustava i aplikacija moraju se redovito primjenjivati.
- Administrativni pristupi webshopu, bazama, cPanelu, hosting sustavu i backupu ograničeni su na ovlaštene osobe.
- Studenti nemaju administrativni pristup webshopu. U pakiranju smiju koristiti samo podatke nužne za pripremu pošiljke i ne smiju ih fotografirati, kopirati, zadržavati niti koristiti u druge svrhe.
- Zaposlenici i studenti obvezni su čuvati povjerljivost i nakon prestanka rada ili angažmana.
- Kod prestanka rada/angažmana pristupi se ukidaju bez odgađanja, vraća se oprema i provjerava prestanak pristupa poslovnim sustavima.

10. Tehničke i organizacijske sigurnosne mjere

- HTTPS/TLS za web komunikaciju i ograničavanje pristupa administrativnim sučeljima.
- Individualni korisnički računi, zaključavanje uređaja i kontrola privilegija.
- Windows Defender i redovito ažuriranje sustava.
- Sigurnosne kopije na Synology sustavu, backup kod hosting providera te dodatna cloud pohrana putem Dropboxa.
- Ograničavanje pristupa MySQL bazama, cPanelu, backupima i datotekama s osobnim podacima.
- Odvajanje produkcijskih i radnih podataka gdje je moguće; zabrana korištenja stvarnih osobnih podataka u testnim okruženjima bez potrebe i odgovarajućih mjera.
- Periodično preispitivanje ovlasti i uklanjanje neaktivnih korisničkih računa.
- Evidentiranje i obrada sigurnosnih incidenata te mogućnost pravodobnog povrata dostupnosti iz sigurnosnih kopija.

Preporuka za daljnje jačanje

Uprava treba tijekom 2026./2027. razmotriti uvođenje 2FA za cPanel, administraciju webshopa, Google/Dropbox račune i druge kritične servise te formalno dokumentirati backup rotaciju i periodični test povrata podataka.

11. Videonadzor

Videonadzor se koristi radi zaštite osoba i imovine u poslovnom prostoru. Snimke se čuvaju 7 dana, osim ako je određena snimka izdvojena zbog incidenta i potrebna kao dokaz u sudskom, upravnom ili drugom odgovarajućem postupku.

- Ulaz u prostor pod videonadzorom mora biti jasno označen propisanom obavijesti prije ulaska u područje snimanja.
- Kamere se postavljaju tako da ne zahvaćaju prostorije za odmor, osobnu higijenu ili presvlačenje te se ne smiju koristiti za nedopušteno praćenje zaposlenika.
- Snimanje javne ili tuđe površine mora biti izbjegnuto; kadar se ograničava na nužni prostor zaštite ulaza, osoba i imovine.
- Pristup snimkama dopušten je samo posebno ovlaštenim osobama, a pristup se evidentira gdje je tehnički izvedivo.

12. Prava ispitanika

Zahtjevi za ostvarivanje prava zaprimaju se putem gdpr@green-tech.hr ili na adresu društva. Društvo provjerava identitet podnositelja u razmjernoj mjeri i postupa u rokovima iz GDPR-a.

- pravo na informacije i pristup osobnim podacima;
- pravo na ispravak netočnih podataka;
- pravo na brisanje kada su ispunjeni uvjeti;
- pravo na ograničenje obrade;
- pravo na prenosivost podataka kada je primjenjivo;
- pravo na prigovor obradi koja se temelji na legitimnom interesu;
- pravo na povlačenje privole bez utjecaja na zakonitost prethodne obrade;
- pravo podnošenja pritužbe Agenciji za zaštitu osobnih podataka (AZOP).

13. Postupanje u slučaju povrede osobnih podataka

Svaki zaposlenik, student ili vanjski suradnik koji primijeti gubitak uređaja, pogrešno slanje podataka, neovlašten pristup, malware, curenje baze, kompromitiran korisnički račun ili drugi sigurnosni incident mora ga bez odgađanja prijaviti Upravi i kontaktu za zaštitu podataka.

1. Zaustaviti ili ograničiti incident i sačuvati dostupne dokaze.
2. Evidentirati datum, vrijeme, sustav, vrste podataka i procijenjeni opseg incidenta.
3. Procijeniti rizik za prava i slobode ispitanika.
4. Ako postoji rizik koji zahtijeva prijavu, obavijestiti AZOP bez nepotrebnog odgađanja i, gdje je izvedivo, u roku od 72 sata od saznanja za povredu.
5. Ako je vjerojatan visok rizik za ispitanike, obavijestiti pogođene osobe jasnim i razumljivim jezikom, osim ako su ispunjeni uvjeti za iznimku.
6. Dokumentirati uzrok, posljedice, poduzete mjere i odluku o tome je li prijava bila potrebna.

14. Evidencija aktivnosti obrade i procjena rizika

Društvo vodi zasebnu Evidenciju aktivnosti obrade prema članku 30. GDPR-a. Evidencija se ažurira pri svakoj značajnoj promjeni svrhe, kategorija podataka, sustava, primatelja, roka čuvanja ili sigurnosnih mjera. Za novu obradu koja može rezultirati visokim rizikom prije početka se procjenjuje potreba za procjenom učinka na zaštitu podataka (DPIA).

15. Edukacija i odgovornost zaposlenika i studenata

- Nove osobe upoznaju se s pravilima povjerljivosti i zaštite osobnih podataka prije dobivanja pristupa podacima.
- Uprava i kontakt za zaštitu podataka organiziraju periodično podsjećanje ili edukaciju, osobito nakon promjena sustava ili incidenta.
- Namjerno neovlašteno korištenje, kopiranje, fotografiranje, prosljeđivanje ili objavljivanje osobnih podataka smatra se ozbiljnim kršenjem internih pravila i može dovesti do radnopравnih i drugih posljedica.

16. Revizija pružatelja i međunarodni prijenosi

Prije ugovaranja novog pružatelja usluge koji može obrađivati osobne podatke društvo provjerava ugovorne uvjete, sigurnosne mjere, lokaciju obrade i uloge strana. Ako se osobni podaci prenose izvan EGP-a, mora postojati odgovarajući mehanizam prijenosa prema GDPR-u, primjerice odluka o primjerenosti ili standardne ugovorne klauzule, uz dodatne mjere kada su potrebne.

17. Završne odredbe

Ovaj Pravilnik stupa na snagu danom donošenja i primjenjuje se na sve organizacijske cjeline, zaposlenike, studente i osobe koje po nalogu društva obrađuju osobne podatke. Uprava je odgovorna za osiguravanje resursa i provedbu, a kontakt za zaštitu podataka koordinira ažuriranja, zahtjeve ispitanika, evidencije i postupanje u incidentima.

Pravilnik se preispituje najmanje jednom godišnje te ranije ako se promijene propisi, poslovni model, informacijski sustavi, kategorije podataka ili procijenjeni rizik obrade.

Za eBurza Grupa d.o.o.

Kontakt za zaštitu podataka

Uprava / direktor

Zvonimir Lisec