PRAVILA POSTUPANJA U OBRADI OSOBNIH PODATAKA U SKLADU SA ČLANKOM 28. OPĆE UREDBE O ZAŠTITI PODATAKA (GDPR)

1. Uvodne odredbe

1. Ovim dokumentom utvrđuju se pravila postupanja povezana sa zaštitom osobnih podataka, te prava i obveze:

- Pravnih i fizičkih osoba koje po nalogu Raiffeisen stambene štedionice d.d. (dalje u tekstu: RSŠ), prilikom isporuka roba i/ili usluga, kao izvršitelji obrade, obrađuju osobne podatke.

2. U ovom Pravilima sljedeći pojmovi imaju pridodano značenje:

"**Izvršitelj obrade**" je pravna ili fizička osoba koja obrađuje osobne podatke u ime druge osobe („Voditelj obrade"), temeljem sklopljenog ugovora.

„**Voditelj obrade**" je pravna ili fizička osoba koja daje nalog Izvršitelju obrade za određenu obradu osobnih podataka.

"Osobni podaci" su svi podaci koji se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi, izravno ili neizravno, osobito uz pomoć podataka kao što su ime, osobni identifikacijski broj (OIB), drugi identifikacijski broj, podaci o lokaciji, mrežni identifikator ili uz pomoć jednog ili više čimbenika svojstvenih za njegov fizički, fiziološki, genetski, mentalni, ekonomski, kulturni ili socijalni identitet

"**Obrada**" je svaki postupak ili skup postupaka koji se obavljaju na osobnim podacima, automatiziranim ili 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

"**GDPR**" (engl. General Data Protection Regulation) je Opća uredba o zaštiti osobnih podataka, punog naziva Uredba (EU) 2016/679 Europskog parlamenta i vijeća od 27. Travnja 2016.g. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ

"**Ispitanik**" je fizička osoba čije osobni podaci se obrađuju temeljem jedne ili više pravnih osnova propisanih GDPR-om. Ispitanik može biti osoba s kojom je

sklopljen ugovor o pružanju pojedine usluge ili je zatražila uslugu, njen/njegov zakonski zastupnik, skrbnik ili punomoćnik, kao i osoba koja je dala privolu za obradu podataka.

"**Privola**" je svako dobrovoljno, posebno, informirano i nedvosmisleno izražavanje želje Ispitanika kojim on izjavom ili jasnom potvrdnom radnjom daje pristanak za obradu osobnih podataka koji se na njega odnose

"**Anonimizacija**" je vrsta obrade osobnih podataka koja uključuje odgovarajuće postupke kojima se onemogućuje identifikacija odnosno povezivanje podataka i/ili zapisa u bazama podataka sa identitetom Voditelja obrade odnosno drugog ispitanika čiji se osobni podaci obrađuju. Anonimizacija se može provesti, primjerice brisanjem podataka ili trajnom izmjenom podataka.

3. Priroda i svrha obrade osobnih podataka koju Izvršitelj obrade vrši za Voditelja obrade navedeni su u pojedinom ugovoru.

4. Izvršenje ugovorene obrade podataka provodit će se isključivo unutar države članice Europske unije (EU) ili unutar države članice Europskog gospodarskog prostora (EEA). Za svaki pojedinačni prijenos podataka u državu koja nije država članica niti EU niti EEA potrebna je prethodna suglasnost Voditelja obrade, a isti će se izvršiti samo ukoliko su ispunjeni posebni uvjeti utvrđeni člankom 44. i dr. Uredbe o zaštiti podataka (Uredba GDPR) te ukoliko je uspostavljena odgovarajuća zaštita na temelju odluke o primjerenosti koju donosi Komisija (čl. 45. Uredbe GDPR) ili putem obvezujućih korporativnih pravila (čl. 46. st. 2. toč. b. zajedno sa čl. 47. Uredbe GDPR), standardnih klauzula o zaštiti podataka (čl. 46. st. 2. toč. c. i d. Uredbe GDPR), odobrenog kodeksa ponašanja (čl. 46. st. 2. toč. e. zajedno sa čl. 40. Uredbe GDPR) i odobrenog mehanizma certificiranja (čl. 46. st. 2. toč. f. zajedno sa čl. 42. Uredbe GDPR), te ostalih mjera kao što su ugovorne klauzule koje odobri tijelo za zaštitu podataka čl. 46. st. 2. toč. a., st. 3. toč. a. i b. Uredbe GDPR) ili odstupanja u posebnim slučajevima definiranim u čl. 49. st. 1. Uredbe GDPR.

5. Vrste osobnih podataka i kategorije ispitanika definirane su u pojedinom ugovoru. U slučaju da u ugovoru nisu navedene vrste podataka i kategorije ispitanika Izvršitelj obrade se obvezuje postupati u skladu s ovim Pravilima sa svim osobnim podacima do kojih je došao ili su mu učinjeni dostupnim za vrijeme trajanja ugovora.

2. Tehničke i organizacijske mjere

1. Prije početka obrade, Izvršitelj obrade je dužan dokumentirati provedbu potrebnih tehničkih i organizacijskih mjera, a takve dokumentirane mjere podnosi Voditelju obrade na uvid. Ukoliko Voditelj obrade uvidom/revizijom utvrdi potrebu za izmjenama tehničkih i organizacijskih mjera, izmjene će se izvršiti temeljem međusobnog dogovora.

2. Izvršitelj obrade uspostavlja sigurnost u skladu sa čl. 28. st. 3. toč. c, a osobito sa čl. 2. Uredbe GDPR zajedno sa čl. 5. st. 1. i st. 2. Uredbe GDPR. Potrebne mjere uključuju mjere sigurnosti podataka te mjere koje jamče odgovarajuću razinu zaštite primjerenu riziku u pogledu povjerljivosti, cjelovitosti, dostupnosti i otpornosti sustava. Pritom se uzimaju u obzir najnovija dostignuća, troškovi implementacije, priroda, područje primjene i svrha obrade te vjerojatnost nastanka povrede i stupanj rizika za prava i slobode pojedinaca u smislu članka 32. st. 1. Uredbe GDPR (detaljnije navedeno u Prilogu 1).

3. Tehničke i organizacijske mjere podložne su tehničkim napretku i daljnjem razvoju. U tom smislu Izvršitelj obrade ima pravo provesti odgovarajuće alternativne mjere. Pritom kod definiranih mjera ne smije doći do smanjenja razine sigurnosti. Sve značajne mjere potrebno je zabilježiti.

3. Obrada podataka isključivo po nalogu Voditelja obrade

1. Izvršitelj obrade i bilo koja druga osoba ovlaštena da djeluje u njegovo ime koja ima pristup osobnim podacima ne smije obrađivati osobne podatke bez zabilježenog odnosno dokumentiranog naloga ili uputa Voditelja obrade, osim u slučaju kada Izvršitelj obrade ima zakonsku obavezu obrađivati osobne podatke.

2. Izvršitelj obrade ne može samostalno ispravljati, brisati ili ograničavati obradu podataka koja se vrši za Voditelja obrade, već to može učiniti isključivo u skladu s dokumentiranim uputama Voditelja obrade. U slučajevima kada ispitanik izravno kontaktira Izvršitelja obrade vezano uz ispravak, brisanje ili ograničenje obrade, Izvršitelj obrade takav zahtjev ispitanika bez odlaganja prosljeđuje Voditelju obrade.

3. Ukoliko nadležno tijelo naloži Izvršitelju obrade da otkrije osobne podatke Voditelja obrade, Izvršitelj obrade će o tome, ukoliko je to zakonski dopušteno, odmah obavijestiti Voditelja obrade, te uputiti nadležno tijelo na Voditelja obrade. Nadalje, Izvršitelj obrade može obrađivati podatke za svoje potrebe isključivo uz pisanu uputu Voditelja obrade.

4. Osiguranje kvalitete i ostale obveze Izvršitelja obrade

1. Osim obveze pridržavanja pravila utvrđenih ugovorom, Izvršitelj obrade je dužan pridržavati se zakonskih obveza propisanih u člancima 28. do 33. Uredbe GDPR; isto tako Izvršitelj obrade će osobito osigurati usklađenost sa sljedećim zahtjevima:
   (a) Pisano imenovanje službenika za zaštitu podataka koji svoje zadaće izvršava u skladu s odredbama članaka 38. do 39. Uredbe GDPR i o tome obavijestiti Voditelja obrade. O bilo kojoj promjeni službenika za zaštitu podataka i/ili njegovih kontakt podataka potrebno je odmah obavijestiti Voditelja obrade. Ukoliko Izvršitelj obrade nema imenovanog službenika za zaštitu podataka, Izvršitelj obrade će Voditelju obrade dati pisano obrazloženje o tome. Ako je RSŠ Izvršitelj obrade podaci o službeniku za zaštitu podataka su dostupni na www.raiffeisenstambena.hr.
   (b) Imenovanje predstavnika u Europskoj uniji ukoliko je Izvršitelj obrade osnovan izvan Europske unije, kako je propisano u članku 27. st. 1. Uredbe GDPR.
   (c) Povjerljivost u skladu sa člankom 28. st. 3. rečenica 2. toč. b, člancima 29. i 32. st. 4. GDPR. Izvršitelj obrade povjerava obradu podataka samo onim zaposlenicima koji su se obvezali na poštivanje povjerljivosti ili koji podliježu zakonskim obvezama o povjerljivosti. Za osobu zaduženu za obradu podataka obveza poštivanja povjerljivosti vrijedi i nakon prestanka zaposlenja i odlaska od Izvršitelja obrade.
   (d) Poduzimanje i pridržavanje svih tehničkih i organizacijskih mjera za potrebe ugovora u skladu sa čl. 28. st. 3. rečenica 2. toč. c, te čl. 32. Uredbe GDPR.
   (e) Prilikom provedbe svojih zadaća Voditelj obrade i Izvršitelj obrade će na zahtjev surađivati s nadzornim tijelima.
   (f) Izvršitelj obrade će Voditelja obrade bez odlaganja obavijestiti o svim kontrolama i mjerama nadzornih tijela ukoliko se odnose na ugovor. To vrijedi i ukoliko se Izvršitelj obrade nalazi pod istragom nadležnih tijela u svezi s upravnopravnim postupkom ili kaznenim postupkom vezano za obradu osobnih podataka u svezi i temeljem ugovora.
   (g) U slučaju da se nad Voditeljem obrade provodi inspekcija nadzornog tijela, upravnopravni postupak, kazneni postupak, spor pokrenut od strane ispitanika ili treće strane radi utvrđivanja odgovornosti ili bilo koji pravni spor vezano uz ugovor temeljem kojeg Izvršitelj obrade vrši obradu podataka, Izvršitelj obrade će poduzeti sve korake kako bi pružio podršku Voditelju obrade.

(h) Dokumentacija i dokaz o tehničkim i organizacijskim mjerama Izvršitelja obrade prema Voditelju obrade u sklopu prava nadzora Voditelja obrade iz članka 6. ovih Pravila.

(i) Izvršitelj obrade je obaviješten da je u postupanju u obradi osobnih podataka temeljem ugovora dužan voditi evidencije aktivnosti obrade kako je propisano člankom 30. Uredbe GDPR. U slučaju da Izvršitelj obrade ne uspostavi evidenciju aktivnosti obrade, Izvršitelj obrade će Voditelju obrade o tome dostaviti obrazloženje u pisanom obliku.

5. Podugovaranje

1. Podugovaranje za potrebe ove odredbe se smatra uslugama koje Izvršitelj obrade ne izvršava sam, već njihovo izvršenje povjerava drugom izvršitelju obrade ("Podugovarač"), a odnose se izravno na pružanje osnovne usluge. To ne uključuje pomoćne usluge, primjerice telekomunikacijske usluge, poštanske ili prijevozničke usluge, održavanje, usluge podrške Voditelju obrade ili uklanjanje nosača podataka, te druge mjere kojima se osigurava povjerljivost, dostupnost, cjelovitost i otpornost sklopovlja i programske podrške koji čine opremu za obradu podataka. Međutim, Izvršitelj obrade ima obvezu sklopiti odgovarajući i pravno obvezujući ugovorni aranžman i poduzeti odgovarajuće mjere inspekcije kojima se osigurava zaštita i sigurnost podataka Voditelja obrade čak i u slučaju eksternalizacije pomoćnih usluga.

2. Izvršitelj obrade može angažirati Podugovarače (dodatne izvršitelje obrade) jedino uz prethodnu izričitu ili dokumentiranu suglasnost Voditelja obrade. Voditelja obrade je potrebno pravovremeno obavijestiti o namjeri angažiranja drugog izvršitelja. Potrebno je osigurati da obveze koje preuzima Podugovarač budu jednake kao obveze kojima podliježe Izvršitelj obrade temeljem ovog ugovora. Ukoliko Podugovarač ne ispuni svoje obveze zaštite podataka, Izvršitelj obrade odgovara Voditelju obrade za ispunjenje obveza podugovarača.

3. Voditelj obrade će izvršiti prijenos osobnih podataka prema Podugovaraču, a Podugovarač će početi obradu podataka tek po ispunjenju svih zahtijeva vezano za podugovaranje.

4. Ukoliko podugovarač pruža ugovorene usluge izvan EU/EEA, Izvršitelj obrade je dužan osigurati usklađenost s Odredbama o zaštiti podataka EU-a provedbom odgovarajućih mjera. Isto vrijedi i ukoliko se koriste pružatelji usluga u skladu sa stavkom 1. rečenicom 2.

6. Pravo nadzora Voditelja obrade

1. Voditelj obrade ima pravo provoditi kontrolu i provjeru sustava za obradu podataka Izvršitelja obrade. Voditelj obrade također može ovlastiti druge osobe za provedbu takve kontrole ili provjere. Izvršitelj obrade može uložiti prigovor na izbor tako ovlaštenih osoba u slučaju opravdanih razloga vezano uz zaposlenika odabrane ovlaštene osobe. Radi izbjegavanja svake sumnje ukoliko je RSŠ Izvršitelj obrade, Voditelj obrade neće imati pravo kontrole sustava RSŠ ako bi to moglo ugroziti sigurnost RSŠ.

2. U slučaju sličnih aktivnosti obrade naloga za nekoliko Voditelja obrade, Izvršitelj obrade dopušta da provjeru izvrše revizori po zajedničkom nalogu takvih voditelja obrade, ili – na zahtjev ili uz suglasnost voditelja obrade – nalaže provedbu odgovarajućih provjera (primjerice od strane internih revizora, vanjskih revizora, revizora za IT sigurnost, revizora za zaštitu podataka, revizora kvalitete), te izvještaje o reviziji dostavlja Voditeljima obrade, njihovim revizorima, a na zahtjev i nadzornim tijelima nadležnim za Voditelje obrade.

3. Izvršitelj obrade jamči da je Voditelj obrade u mogućnosti potvrditi usklađenost s obvezama Izvršitelja obrade u skladu sa člankom 28. Uredbe GDPR i ovim ugovorom. Izvršitelj obrade će Voditelju obrade dostaviti sve podatke potrebne za potvrđivanje usklađenosti Izvršitelja obrade sa svojim obvezama, osobito s obvezom provedbe tehničkih i organizacijskih mjera.

4. Dokaz o provedbi takvih mjera koje se tiču ne samo pojedinog ugovora, moguće je pružiti u obliku
   - Potvrde usklađenosti s odobrenim kodeksom ponašanja u skladu sa člankom 40. Uredbe GDPR;
   - Certifikata prema odobrenoj proceduri certificiranja u skladu sa člankom 42. Uredbe GDPR; ili
   - Važećih certifikata revizora ili izvještaja neovisnih tijela (revizor, revizor za IT sigurnost, revizor za privatnost podataka, revizor kvalitete).

7. Obveza Izvršitelja obrade za pružanje pomoći

1. Izvršitelj obrade će Voditelju obrade pružati pomoć prilikom ispunjavanja obveza u pogledu sigurnosti osobnih podataka, obveza izvještavanja o povredama zaštite podataka, procjena učinka na zaštitu podataka te prethodnih konzultacija propisanih u člancima 32. do 36. Uredbe GDPR. To se odnosi na:

(a) osiguranje odgovarajuće razine zaštite provedbom tehničkih i organizacijskih mjera koje u obzir uzimaju okolnosti i svrhu obrade kao i procijenjenu vjerojatnost i ozbiljnost mogućih povreda zakona uslijed ranjivosti u pogledu sigurnosti, i koje omogućuju hitno utvrđivanje takvih slučajeva povreda ,
(b) obvezu hitnog obavješćivanja Voditelja obrade o povredi osobnih podataka;
(c) dužnost pružanja pomoći Voditelju obrade u vezi ispunjavanja obveze Voditelja obrade pružanja informacija ispitaniku i hitnog pružanja svih relevantnih podataka Voditelju obrade u tom pogledu;
(d) pomaganje Voditelju obrade u procjeni učinka na zaštitu podataka i
(e) pomaganje Voditelju obrade vezano uz prethodne konzultacije s nadzornim tijelima.

2. Izvršitelj obrade je dužan pomagati Voditelju obrade u pogledu tehničkih i organizacijskih mjera, kako bi Voditelj obrade u bilo kojem trenutku bio u mogućnosti poštivati prava ispitanika utvrđenih u Poglavlju III Uredbe GDPR (pravo na informacije, pristup, ispravak i brisanje osobnih podataka, prenosivost podataka, prigovor i automatizirano pojedinačno donošenje odluka) u zakonskom roku, i Izvršitelj obrade će u tu svrhu Voditelju obrade pružiti sve potrebne informacije. Ukoliko Izvršitelju obrade bude upućen odgovarajući zahtjev koji pokazuje da podnositelj zahtjeva pogrešno smatra da je Izvršitelj obrade Voditelj obrade podataka kojima upravlja, Izvršitelj obrade će bez odlaganja takav zahtjev proslijediti Voditelju obrade i o tome obavijestiti podnositelja zahtjeva.

3. Osim ukoliko nije drugačije ugovoreno, Izvršitelj obrade je prema dokumentiranoj zabilježenoj uputi Voditelja obrade dužan osigurati brisanje podataka, pravo na zaborav, ispravak podataka, prenosivost podataka i pravo pristupa.

8. Ovlaštenje Voditelja obrade za davanje uputa

1. Voditelj obrade će usmene upute bez odlaganja potvrditi i pisanim putem (dovoljno je slanje elektronske poruke).

2. Izvršitelj obrade će Voditelja obrade bez odlaganja obavijestiti ukoliko smatra da se uputom krše odredbe o zaštiti podataka. Izvršitelj obrade u tom slučaju ima pravo obustaviti izvršenje takve upute sve dok Voditelj obrade istu ne potvrdi ili izmijeni.

9. Brisanje i povrat osobnih podataka

1. Kopije ili duplikati podataka ni u kom se slučaju ne mogu izrađivati bez znanja Voditelja obrade, osim sigurnosnih kopija ukoliko su iste potrebne radi osiguranja uredne obrade podataka i podataka potrebnih za ispunjenje zakonskih obveza vezano za čuvanje podataka.

2. Nakon sklapanja ugovorenog posla, ili ranije na zahtjev Voditelja obrade, a najkasnije po prestanku važenja ugovora o pružanju usluge, Izvršitelj obrade će Voditelju obrade predati svu dokumentaciju koju bude posjedovao, sve rezultate obrade ili korištenja, te sve skupove podataka vezano uz ugovor, bez zadržavanja bilo kakvih kopija, bez obzira na suprotne pravne zahtjeve; ili, kao alternativa, Izvršitelj obrade će, uz prethodnu suglasnost Voditelja obrade, obrisati ili na drugi način uništiti svu takvu dokumentaciju, rezultate obrade ili korištenja, te sve skupove podataka, uz poštivanje obveza zaštite podataka, na način da postoji mogućnost potvrde uništenja ili brisanja podataka, ali bez mogućnosti poništenja istog. Isto vrijedi i na sve povezane testne, otpadne, nepotrebne i odbačene materijale. Dokaz uspješnog uništenja ili brisanja podataka daje se na zahtjev. Ukoliko Izvršitelj obrade obrađuje podatke u posebnom tehničkom formatu, podatke će predati ili u tom obliku ili, na zahtjev Voditelja obrade, u obliku u kojem je podatke dobio od Voditelja obrade, ili u bilo kojem drugom uobičajenom obliku nakon prestanka važenja ugovora.

3. Dokumentaciju koja se koristi u svrhu dokazivanja uredne obrade podataka u skladu s ugovorom Izvršitelj obrade će čuvati i nakon isteka roka važenja ugovora u skladu s odgovarajućim rokovima za čuvanje podataka. Izvršitelj obrade može takvu dokumentaciju predati Voditelju obrade na kraju roka važenja ugovora kako bi Izvršitelj obrade bio oslobođen ove obveze.

10. Ostale odredbe

1. Ukoliko dođe do ugrožavanja podataka ispitanika koje vodi Izvršitelj obrade kao posljedica provedbe ovrhe ili zaplijene, stečajnog postupka ili bilo kojih drugih događaja ili mjera koje provodi treća strana, Izvršitelj obrade će o tome bez odlaganja obavijestiti Voditelja obrade. Izvršitelj obrade će bez odlaganja obavijestiti sve odgovarajuće i nadležne institucije ili osobe da Voditelj obrade kao Voditelj obrade kako je definirano Uredbom GDPR ima isključivu nadležnost i pravo vlasništva nad podacima.

2. RSŠ može usvojiti izmjene i dopune ovih Pravila i svih njihovih priloga. Sve izmjene i dopune Pravila RSŠ će objaviti na www.raiffeisenstambena.hr.

3. Izvršitelj obrade se obvezuje poštivati obveze čuvanja bankovne tajne u skladu sa člankom 157. Zakona o kreditnim institucijama u odnosu na sve podatke o strankama Voditelja obrade koji budu proslijeđeni, dostavljeni ili poznati Izvršitelju obrade tijekom ispunjenja naloga ili pružanja usluga. Nadalje, Izvršitelj obrade će sve svoje djelatnike i druge osobe ovlaštene temeljem naloga ili pružanjem usluga obvezati na čuvanje bankovne tajne te poduzeti korake da isti poštuju bankovnu tajnu.

11. Stupanje na snagu

1. Ova Pravila stupaju na snagu 25. svibnja 2018.

Prilog 1
Tehničke i organizacijske mjere

1. Povjerljivost (članak 32 st. 1 toč. b Uredbe GDPR)

- **Kontrola fizičkog pristupa**
  Zaštita od neovlaštenog pristupa opremi za obradu podataka, npr. magnetske ili chip kartice, ključevi, elektronsko otvaranje vrata, zaštitarsko osoblje, portir, alarmni sustavi, video/CCTV sustavi;
- **Kontrola elektronskog pristupa**
  Zaštita od neovlaštenog korištenja sustava za obradu i pohranjivanje podataka, npr. (sigurnosne) zaporke (uključujući primjenu odgovarajuće politike), mehanizmi automatskog blokiranja/zaključavanja, dvofaktorska autentifikacija, enkripcija nositelja podataka/medija za pohranu podataka;
- **Kontrola internog pristupa**
  Sprečavanje neovlaštenog čitanja, kopiranja, promjene ili brisanja podataka unutar sustava, npr. standardni profili ovlaštenja osoba kojima je to nužno iz poslovnih razloga (need-to-know princip), standardne procedure za dodjelu ovlaštenja, vođenje dnevnika pristupa (access log), periodički pregled dodijeljenih ovlaštenja, uključujući između ostalog i administrativne korisničke račune;
- **Kontrola zasebne obrade**
  Zasebna obrada podataka koji se prikupljaju za različite potrebe, npr. podrška za više klijenata, *sandboxing*;
- **Pseudonimizacija** (članak 32 st. 1 toč. a Uredbe GDPR; članak 25 st. 1 Uredbe GDPR)
  Ukoliko je potrebno ili uputno za potrebe odgovarajućih aktivnosti obrade podataka, primarna identifikacijska obilježja osobnih podataka uklanjaju se iz aplikacije za obradu podataka kako se podaci ne bi mogli povezati s

pojedinim ispitanikom bez korištenja dodatnih informacija, pod uvjetom da se te dodatne informacije zasebno čuvaju i podliježu odgovarajućim tehničkim i organizacijskim mjerama.

- **Shema klasifikacije podataka**
  Poštivanje modela za klasifikaciju podataka koju provodi Voditelj obrade (npr. tajno/povjerljivo/interno/javno);
- **Kontrole koncepcije tehničkog brisanja**
  Za podatke i meta podatke, primjerice log datoteke itd.;

2. 2. Cjelovitost (članak 32 st. 1 toč. b Uredbe GDPR)

- **Kontrola prijenosa podataka**
  Sprečavanje neovlaštenog čitanja, kopiranja, promjene ili brisanja podataka tijekom elektronskog prijenosa ili transporta, npr. enkripcija, virtualne privatne mreže (VPN), elektronski potpis;
- **Kontrola unosa podataka**
  Provjera vrši li se, i od strane koga, unos, promjene ili brisanje osobnih podataka u sustavu za obradu podataka, npr.: evidentiranje, upravljanje dokumentima;

3. Dostupnost i otpornost (članak 32 st. 1 toč. b Uredbe GDPR)

- **Kontrola dostupnosti**

Sprečavanje slučajnog ili namjernog uništavanja ili gubitka podataka, npr. strategija izrade sigurnosnih-backup kopija (online/offline; on-site/off-site), sustav neprekidnog napajanja (UPS, diesel agregat), antivirusni program, vatrozid, procedure prijavljivanja i interventni planovi postupanja u izvanrednim situacijama; sigurnosne provjere na razini infrastrukture i aplikacija, multi-stage backup concept uključujući šifriranu eksternalizaciju sigurnosnih kopija u backup podatkovni centar, standardne procedure za slučajeve promjene zaposlenika ili odlaska iz poduzeća

- **Brzi oporavak** (članak 32 st. 1 toč. c Uredbe GDPR);

4. Procedure za redovno testiranje, ocjenjivanje i procjenjivanje (članak 32 st. 1 toč. d Uredbe GDPR; članak 25 st. 1 Uredbe GDPR)

- Upravljanje zaštitom podataka, uključujući redovitu edukaciju djelatnika;
- Procedure za odgovor na sigurnosne incidente;
- Tehnička i integrirana zaštita podataka (članak 25. st. 2. Uredbe GDPR);
- Kontrola ugovora
  U skladu sa člankom 28. Uredbe GDPR nije dopuštena obrada podataka bez odgovarajućih uputa Voditelja obrade, npr. jasni i jednoznačni ugovorni aranžman, formalizirano Upravljanje nalozima, stroge kontrole odabira pružatelja usluge, obveza prethodne procjene, naknadne kontrolne provjere.