

Varstvo osebnih podatkov

E-izobraževanje Kreditni posredniki



Namen in cilj

Namen izobraževanja je preprečiti kršitev ureditve na področju varstva osebnih podatkov ter neupravičeno obdelavo osebnih podatkov s strani kreditnih posrednikov.

Cilj izobraževanja je zaposlenim pri kreditnem posredniku pojasniti ureditev področja varstva osebnih podatkov in njihove odgovornosti v zvezi z ravnanjem z osebnimi podatki.

Uvod

- Pravica do varstva zasebnosti in pravica do varstva posameznikov pri obdelavi osebnih podatkov je temeljna pravica.
- S **25. majem 2018** je stopila v veljavo splošna uredba EU, tako imenovana **GDPR**, ki ureja področje varstva osebnih podatkov na območju celotne Evropske unije (»EU«) in se neposredno uporablja tudi pri nas. Poleg uredba imamo še Zakon o varstvu osebnih podatkov (ZVOP-2), ki ureja področja, ki jih sama uredba ni uredila (npr. videonadzor, biometrija) in daje podlago Informacijskemu pooblaščenču za izrekanje sankcij po GDPR.



Kaj je **podatek**?



OSEBNI PODATEK je katerikoli podatek oziroma informacija, ki se nanaša na določenega ali določljivega posameznika. Ko v banki govorimo o osebnih podatkih velja to tako za osebne podatke o komitentih, nekomitentih in zaposlenih s katerimi se lahko srečamo pri našem poslovanju.

Vi se boste srečevali z osebnimi podatki strank, ki so lahko komitenti ali nekomitenti (bodo postali stranke banke).

Osebni podatki so podatki, ki:

- omogočajo identifikacijo posameznika (ime in priimek oz. drug znak, fotografija ipd.) in
- o njem nekaj povedo (kakšen je njegov status, kje se nahaja ipd.).

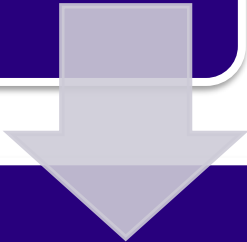
Posameznika identificirate neposredno:

- s pomočjo njegovih identifikacijskih števil (npr. EMŠO, davčna številka, številka zdravstvenega zavarovanja, telefonska).

-

Kaj je **obdelava** osebnih podatkov?

Obdelava osebnih podatkov pomeni **vsako dejanje, ki se izvaja z osebnimi podatki**. Za obdelavo osebnih podatkov šteje že samo *zbiranje* podatkov, kot tudi njihovo beleženje - vpis, urejanje, shranjevanje, prilagajanje ali spreminjanje, priklicanje, **vpogled**, uporabo, razkritje s prenosom, sporočanje, širjenje ali drugo dajanje na razpolago, razvrstitev ali povezovanje, blokiranje, anonimiziranje, izbris ali uničenje.



Posrednik obdeluje osebne podatke za namen sklenitve kredita na prodajnem mestu.

Kaj so **osnovna načela** pri varstvu osebnih podatkov?

OSNOVNA NAČELA, ki jih je potrebno upoštevati pri obdelavi osebnih podatkov:

1. **Zakaitost, pravičnost in preglednost** –

Obdelava je zakonita, če jo **določa zakon** ali če je za obdelavo podana **osebna privolitev posameznika**. V zasebnem sektorju, se osebni podatki lahko med drugim obdelujejo v primeru, ko na podlagi povpraševanja posameznika sklepamo kreditno pogodbo.

2. **Omejitev namena** – namen obdelave mora biti določen in zakonit – obdelovanje osebnih podatkov mora torej imeti podlago v zakonu ali privolitvi posameznika

3. **Najmanjši obseg podatkov** – zbiranje osebnih podatkov **ni prekomerno glede na namen**. Za namene sklepanja kreditnih poslov so vsi podatki, ki jih vnašate v aplikacijo »NLB krediti na prodajnih mestih« zakonsko potrebni.

Točnost (in ažurnost) – Točnost podatkov ni enaka ažurnosti podatkov: točnost pomeni, da so podatki pravilni in popolni, ažurnost pa pomeni, da se uporablja zadnji, v tem trenutku veljaven podatek. Npr.: zaradi spremembe naslova stranke, ki vam ga ponudi aplikacija za stranko NLB, **moramo popraviti netočne podatke**.

4. **Omejitev shranjevanja** – osebni podatki se lahko shranjujejo le toliko časa, dokler je to potrebno za doseg namena (10 let po zaključku poslovnega razmerja).

5. **Celovitost in zaupnost** – zagotavljati je potrebno varovanje podatkov z namenom preprečevanja nepooblaščne obdelave osebnih podatkov.

6. **Odgovornost** – med drugim pomeni obveščanje o varnostnih incidentih, izvajanje varnostnih ukrepov, idr.



Kdaj lahko **obdelujemo** osebne podatke?

Posredniki so pogodbeni upravljalci za banko in velja enako kot za banko in sicer lahko osebne podatke obdeluje le, če za to obstoji ustrezna pravna podlaga, ki je v primeru potrošniških kreditov:

- **Zakon o bančništvu,**
- **zakon, ki ureja preprečevanje pranja denarja in financiranja terorizma,** ki banki nalaga izvajanje ukrepa prepoznavne stranke, s katerim se preverja istovetnosti stranke, in sicer izrecno pri sklepanju poslovnega razmerja. Banka osebne podatke stranke pridobi neposredno od stranke in z vpogledom v njen uradni osebni dokument.
- **zakon, ki ureja potrošniške kredite** nalaga, da pred sklenitvijo kreditne pogodbe s potrošnikom oceni njegovo kreditno sposobnost. Ta se opravi na podlagi informacij o prihodkih in izdatkih oziroma premoženjskem stanju potrošnika, ki jih banka pridobi od potrošnika in iz centralnega kreditnega registra oziroma sistema SISBON – navedeno obdelavo SISBON izvaja banka in ne posrednik.
- **pogodba,** velik del osebnih podatkov banka obdeluje tudi na pogodbeni podlagi, saj pogodbe in obveznosti banke, ki izhajajo iz kreditne pogodbe, brez tega ne bi bilo moč izvajati.



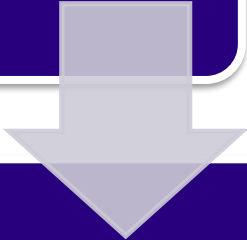
Kako mora vsak od nas **varovati** osebne podatke?



- Za varstvo osebnih podatkov poskrbimo tako, da:
 - ne izvajamo nepooblaščenih obdelav podatkov (npr.: neupravičen vpogled, neupravičeno posredovanje, obdelava brez ustrezne pravne podlage);
 - podatke varujemo pred nenamernim ali nezakonitim uničenjem, izgubo, spremembami in drugimi zlorabami;
 - redno in sproti brišemo ali uničujemo podatke, ko jih ne potrebujemo več oz. jim je potekel rok hrambe in sicer tako v papirni, kot tudi v elektronski obliki;
 - ne razkrivamo osebnih podatkov nepooblaščenim osebam;
-
-
- Kako varujemo osebne podatke?
-
- Kreditni posrednik mora varnost osebnih podatkov zagotavljati z doslednim izvajanjem naslednjih pravil:
 - zaklepamo prostore, omare in predale,
 - zaklepamo računalnik, ko nismo prisotni,
 - zavarujemo podatke pri njihovem elektronskem prenosu (šifriranje),
 - učinkovito uničujemo nepotrebne podatke na papirnih in elektronskih nosilcih,
 - upoštevamo pravila za varno ravnanje in izbiro gesel,
 - z vso skrbnostjo se trudimo prepoznati socialni inženiring.

Posledice neustreznega izvajanja varovanja osebnih podatkov

nezakonita obdelava, nepooblaščno razkritje, izguba ali zloraba osebnih podatkov lahko povzroči izgubo zaupanja strank in ugleda NLB ter odgovornost za nastanek morebitne škode, ki bi posamezniku, na katerega se nanašajo podatki, ob tem nastala



zaradi neprimerne varovanja osebnih podatkov smo odgovorni za kršitev predpisov in se nam lahko izreče globa, globa se lahko izreče NLB in zaposlenemu pri posredniku, ki je kršil svoje obveznosti glede varstva osebnih podatkov.

Kaj moramo storiti, če **zaznamo** kršitev varstva osebnih podatkov?



Vsak zaposleni pri posredniku je dolžan nemudoma poročati o kršitvi varstva osebnih podatkov!

Komu moramo poročati kršitve varstva osebnih podatkov?

Sporočimo jih nemudoma **kontaktni osebi pri posredniku**, ki mora nemudoma poročati naprej NLB.

Na kakšen način poročamo o kršitvi varstva osebnih podatkov?

Sporočimo jih preko:

- elektronske pošte, ki je določena pri posredniku

Kaj mora vsebovati obvestilo o kršitvi?

Obvestilo o kršitvi varstva osebnih podatkov mora vsebovati najmanj naslednje informacije:

- datum in čas kršitve varstva osebnih podatkov,
- kraj kršitve varstva osebnih podatkov,
- opis kršitve varstva osebnih podatkov,
- ime in priimek osebe, ki je zaznala kršitev varstva osebnih podatkov.

Po GDPR je obvezno poročanje nadzornemu organu (Informacijski pooblaščenec Republike Slovenije) o incidentih, katerih posledica je ogrožanje zaupnosti osebnih podatkov v 72 urah (npr. nepooblaščena obdelava osebnih podatkov, izguba podatkov, kraja podatkov), pri večjih incidentih pa tudi obveznost obveščanja posameznikov.

Revizijska sled

Informacijski sistem beleži vse dostope (tudi vpogled) do osebnih podatkov, s katerimi upravlja NLB. Beleženje dostopov omogoča naknadno preverjanje, kdo, kdaj in do katerih osebnih podatkov je dostopal.

Banka lahko revizijsko sled uporablja v primerih postopkov reševanja varnostnih incidentov in v postopkih nadzora poslovne upravičenosti obdelav osebnih podatkov.

Primeri nedopustnega ravnanja oz. kršitve varovanja osebnih podatkov

Primeri **nedopustnega ravnanja** z osebnimi podatki:

1. Sodelavka, ki nima dostopa do aplikacije, me prosi, da v aplikaciji »NLB krediti na prodajnih mestih« pogledam naslov stranke. Ker gre za enkraten dogodek, brez skrbi pridobim podatek iz aplikacije.
2. Ker vem, da je prijatelju stranka, ki sem ji urejal kredit vseč, naredim s telefonom sliko ekrana v aplikaciji »NLB krediti na prodajnih mestih« kjer je razviden naslov stranke.





POMEMBNO!

Kreditni posredniki razpolagamo s pooblastili za dostop in posledično obdelavo osebnih podatkov strank. Pooblastila so nam dodeljena z namenom izvajanja sklepanja kreditnih pogodb, kar pa **ne pomeni**, da v osebne podatke lahko vpogledujemo tudi iz radovednosti, lastnega interesa ali z namenom posredovanja osebnih podatkov znancu ali drugi nepooblaščenim osebam.

Vpogledovanje v osebne podatke brez ustrezne pravne podlage (brez poslovne potrebe), je strogo prepovedano. Do takih dejanj imamo v NLB ničelno toleranco.

Upoštevajoč določila GDPR mora banka vse ugotovljene oziroma potrjene primere obdelave osebnih podatkov brez ustrezne pravne podlage, javiti Informacijskemu pooblaščenцу Republike Slovenije. Le-ta lahko v skladu s svojimi pristojnostmi posamezniku, ki je nepooblaščen obdeloval osebne podatke izreče kazen v obliki plačila globe ali celo poda kazensko ovadbo organom pregona.

Pravice, ki jih ima posameznik v zvezi s svojimi osebnimi podatki



- NLB posameznikom – strankam, na katere se nanašajo osebni podatki, omogoča uresničevanje naslednjih pravic: pravice do dostopa do osebnih podatkov in popravka ali izbrisa osebnih podatkov, pravice do omejitve obdelave, pravice do prenosljivosti ter uresničevanje pravice do ugovora.
- Posameznika, ki bi želel uveljavljati pravice po GDPR usmerite na Pooblaščenca za varstvo osebnih podatkov, ki ga stranka lahko kontaktira na elektronski naslov dpo@nlb.si