



Splošna uredba o varstvu podatkov: nove priložnosti, nove obveznosti



Kaj mora vsako **podjetje** vedeti o splošni
uredbi EU o varstvu podatkov

Printed by Bietlot in Belgium

Niti Evropska komisija niti osebe, ki delujejo v njenem imenu, niso odgovorne za uporabo podatkov iz te publikacije.

Luxembourg: Urad za publikacije Evropske unije, 2018

© Evropska unija, 2018

Ponovna uporaba je dovoljena z navedbo vira.

Politiko ponovne uporabe dokumentov Evropske komisije ureja Sklep 2011/833/EU (UL L 330, 14.12.2011, str. 39).

Print ISBN 978-92-79-79444-5 doi:10.2838/34760 DS-01-18-082-SL-C

PDF ISBN 978-92-79-79413-1 doi:10.2838/96353 DS-01-18-082-SL-N

KAZALO

POGLAVJE 1

POSLOVNA PRILOŽNOST 2

POGLAVJE 2

RAZUMEVANJE SPLOŠNE UREDBE O VARSTVU PODATKOV 4

POGLAVJE 3

VAŠE OBVEZNOSTI NA PODLAGI SPLOŠNE UREDBE
O VARSTVU PODATKOV 8

POGLAVJE 4

STE PRIPRAVLJENI IZPOLNITI OBVEZNOST? 18



POGLAVJE 1

POSLOVNA PRILOŽNOST

Splošna uredba o varstvu podatkov ureja, kako podjetja obdelujejo osebne podatke in ravnajo z njimi. Veljati začne 25. maja 2018, uporablja pa se za vsa podjetja in organizacije (npr. bolnišnice, javno upravo itd.) ter pomeni največjo spremembo v predpisih EU o varstvu podatkov po več kot dvajsetih letih.

Državljanom ne omogoča samo več nadzora nad tem, kako se njihovi osebni podatki uporabljajo, temveč tudi močno poenostavlja zakonodajno okolje za podjetja,

saj vzpostavlja enoten zakonodajni okvir za varstvo podatkov po vsej EU. Namesto da bi imela vsaka država svoje zakone o varstvu podatkov, bo to področje v celotni EU zdaj urejala ena sama uredba. Podjetju, ki posluje v različnih državah, ne bo več treba izpolnjevati številnih in pogosto tudi različnih predpisov. Če bo želelo kjer koli v EU ponujati svoje storitve, bo moralo izpolnjevati samo obveznosti iz splošne uredbe o varstvu podatkov.

Kako lahko splošna uredba o varstvu podatkov koristi vašemu podjetju

- 🏠 **Ena Unija, ena zakonodaja:** poslovanje podjetij v EU je z enim samim sklopom predpisov enostavnejše in cenejše.
- 🏠 **Vse na enem mestu:** večinoma imajo podjetja opravka s samo enim organom za varstvo podatkov.
- 🏠 **Evropski predpisi na evropskih tleh:** podjetja, ki imajo sedež zunaj EU, morajo uporabljati iste predpise kot evropska podjetja, kadar ponujajo blago ali storitve osebam v EU.
- 🏠 **Pristop na podlagi tveganja:** splošna uredba o varstvu podatkov se ogiba obremenjujočim obveznostim, ki so enake za vse, in namesto tega obveznosti prilagaja določenim tveganjem.
- 🏠 **Predpisi, primerni za inovacije:** splošna uredba o varstvu podatkov je tehnološko nevtralna.

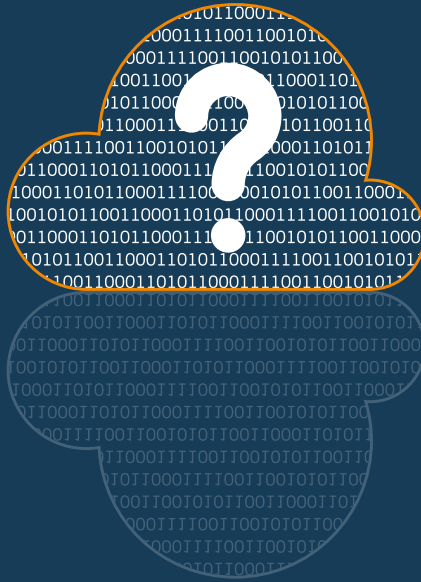
Gre za zaupanje

Varstvo osebnih podatkov je za posameznike pomembno, njihovo zaupanje v digitalno okolje pa je še vedno na nizki ravni. Raziskava Eurobarometra je pokazala, da:

- 🏠 osem ljudi od desetih meni, da nimajo popolnega nadzora nad svojimi osebnimi podatki,
- 🏠 šest ljudi od desetih pravi, da ne zaupajo spletnim podjetjem,
- 🏠 več kot 90 % Evropejcev želi enake pravice glede varstva podatkov v vseh državah EU.

Splošna uredba o varstvu podatkov daje z upravljanjem osebnih podatkov na podlagi tveganja vašemu podjetju novo priložnost za povečanje zaupanja potrošnikov.

„Podjetja, ki ne zagotavljajo ustreznega varstva osebnih podatkov posameznikov, tvegajo, da bodo izgubila zaupanje potrošnikov, ki pa je pomembno, če želijo ljudi spodbuditi k uporabi novih proizvodov in storitev.“



POGLAVJE 2

RAZUMEVANJE SPLOŠNE UREDBE O VARSTVU PODATKOV

Ali splošna uredba o varstvu podatkov velja zame?

Splošna uredba o varstvu podatkov velja za **vsako** podjetje, ki:

obdeluje osebne podatke z avtomatiziranimi sredstvi ali **ročno** (pod pogojem, da so podatki razvrščeni v skladu z merili).

Predpise morate upoštevati tudi, če vaše podjetje zgolj obdeluje podatke v imenu drugih podjetij.

Splošna uredba o varstvu podatkov se uporablja, če:

- 📍 vaše podjetje obdeluje osebne podatke in ima sedež v EU, ne glede na to, kje se dejanska obdelava podatkov izvaja, ali
- 📍 če ima vaše podjetje sedež zunaj EU, vendar ponuja blago ali storitve posameznikom v EU ali spremlja njihovo vedenje.

Kaj so osebni podatki

Osebni podatki so katera koli informacija v zvezi z določenim ali določljivim živim posameznikom. Vključujejo lahko:

- 📍 ime in priimek,
- 📍 naslov in telefonsko številko,
- 📍 lokacijo,
- 📍 podatke o zdravstvenem stanju,
- 📍 podatke o dohodku in bančne podatke,
- 📍 kulturne preference
- 📍 in še veliko več.

Na področje uporabe splošne uredbe o varstvu podatkov spadajo tudi osebni podatki, ki jih je treba deidentificirati

ali psevdonimizirati, vendar se še vedno lahko uporabijo za ponovno identifikacijo osebe. Za osebne podatke pa ne štejejo več tisti podatki, ki so nepreklicno anonimizirani tako, da posameznik ni več določljiv, zato jih splošna uredba o varstvu podatkov ne ureja.

Splošna uredba o varstvu podatkov je tudi tehnološko nevtralna, kar pomeni, da varuje osebne podatke, ne glede na to, katera tehnologija se uporablja ali kako so osebni podatki shranjeni. Z uredbo se urejajo vaši postopki, pa naj vaše podjetje obdeluje ali shranjuje osebne podatke s pomočjo kompleksnega sistema IT ali v obliki evidenc v papirni obliki.

„Z uredbo se urejajo vaši postopki, pa naj vaše podjetje obdeluje ali shranjuje osebne podatke s pomočjo kompleksnega sistema IT ali v obliki evidenc v papirni obliki.“

Posebej pozorno ravnajte s posebnimi (občutljivimi) kategorijami osebnih podatkov

Osebni podatki, ki jih zbirate, veljajo za občutljive, kadar vključujejo informacije o zdravju, rasi, spolni usmerjenosti, veroizpovedi, političnih prepričanjih ali članstvu v sindikatu. Vaše podjetje sme obdelovati te podatke samo pod določenimi pogoji, pri čemer boste morda morali izvajati dodatne zaščitne ukrepe, npr. šifriranje.

Kaj je obdelava osebnih podatkov

Pojem obdelave osebnih podatkov v skladu s splošno uredbo o varstvu podatkov zajema dejanja, kot so zbiranje, uporaba in izbris osebnih podatkov.

Ali nadzorujete svoje prostore z nadzorno kamero? Ali pregledujete zbirko osebnih podatkov za poslovne namene? Ali pošiljate promocijsko elektronsko pošto?

Brišete (digitalne) datoteke o zaposlenih ali uničujete dokumente? Ste morda objavili fotografijo osebe na svojem spletnem mestu ali kanalih družbenih medijev?

Če ste na katero koli od teh vprašanj odgovorili pritrdilno, potem vaše podjetje zagotovo obdeluje osebne podatke.

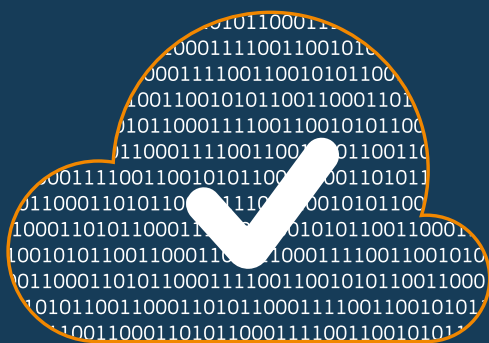
Kako vam splošna uredba o varstvu podatkov pomaga zmanjšati stroške

Splošna uredba o varstvu podatkov upošteva potrebe podjetij. Cilj uredbe je npr. odpraviti upravne zahteve, da bi se zmanjšali stroški in upravno breme:

- 📌 **brez vnaprejšnjih obvestil:** reforma odpravlja vnaprejšnja obvestila za nadzorne organe, skupaj z njihovimi stroški;
- 📌 **pooblaščen osebe za varstvo podatkov:** podjetja morajo imenovati pooblaščen osebo za varstvo podatkov zlasti, kadar njihove temeljne dejavnosti vključujejo obdelavo občutljivih podatkov v velikem obsegu ali redno in sistematično spremljanje posameznikov v velikem obsegu. Javne uprave so dolžne imenovati pooblaščen osebo za varstvo podatkov;

- 📌 **ocene učinka v zvezi z varstvom podatkov:** podjetja morajo izvajati ocene učinka v zvezi z varstvom podatkov samo, če predlagana dejavnost obdelave podatkov vključuje veliko tveganje za pravice in svoboščine posameznikov;
- 📌 **vodenje evidenc:** podjetja z manj kot 250 zaposlenimi niso dolžna voditi evidence, razen če je obdelava podatkov naključna ali vključuje občutljive informacije.

„Cilj uredbe je npr. odpraviti upravne zahteve, da bi se zmanjšali stroški in upravno breme.“



POGLAVJE 3

VAŠE OBVEZNOSTI NA PODLAGI SPLOŠNE UREDBE O VARSTVU PODATKOV

Splošna uredba o varstvu podatkov določa neposredne obveznosti glede obdelave podatkov na ravni celotne EU. Podjetja smejo v skladu z uredbo obdelovati osebne podatke samo pod določenimi pogoji. Obdelava mora biti npr. poštena in pregledna, izvajati se mora za določen in zakonit namen in biti omejena samo na podatke, potrebne za ta namen. Utemeljena mora biti na eni izmed naslednjih pravnih podlag:

- 👤 **privolitev** zadevnega posameznika,
- 👤 **pogodbena obveznost** med vami in posameznikom,
- 👤 izpolnjevanje **pravne obveznosti**,
- 👤 zaščita življenjskih interesov posameznika,
- 👤 izvajanje **naloge v javnem interesu**,
- 👤 **zakoniti interesi** vašega podjetja, vendar šele po tem, ko ste preverili, da to nima resnega vpliva na temeljne pravice in svoboščine posameznika, čigar podatke obdelujete. Če pravice osebe prevladajo nad vašimi interesi, podatkov ne smete obdelovati.

V središču: pridobitev privolitve za uporabo osebnih podatkov

Splošna uredba o varstvu podatkov uporablja stroga pravila za obdelavo podatkov na podlagi privolitve. Namen teh predpisov je zagotoviti, da posameznik razume, v kaj je privolil. To pomeni, da mora biti privolitev **prostovoljna, izrecna, informirana** in **nedvoumna** ter dana na podlagi zahtevka v jasnem in preprostem jeziku. Poleg tega mora biti dana tudi s **pritrtilnim dejanjem**, npr. na spletu z označitvijo polja ali s podpisom obrazca.

Če na podlagi privolitve obdelujete osebne podatke o **otroku**, se zahteva privolitev staršev. Ker pa starostna omejitev v različnih državah sega od 13 do 16 let, vam svetujemo, da preverite nacionalno zakonodajo.

*Ne pozabite!
Ko oseba privoli
v obdelavo svojih osebnih
podatkov, lahko te podatke
obdelujete samo za namene,
za katere je bila privolitev dana. Poleg
tega morate tej osebi omogočiti tudi, da
svojo privolitev prekliče.*

Določite svojo vlogo in odgovornosti

Ko se pripravate, da splošna uredba o varstvu podatkov velja za vaše podjetje in da vaše dejavnosti vključujejo obdelavo osebnih podatkov, morate določiti svojo vlogo.

Predpisi o varstvu podatkov razlikujejo med upravljavcem in obdelovalcem podatkov, ki imata različne obveznosti. Medtem ko upravljavec podatkov določi namen in sredstva za obdelavo osebnih podatkov, je obdelovalec tisti, ki osebne podatke obdeluje v imenu upravljavca podatkov. Vendar to ne pomeni, da se obdelovalec lahko preprosto skrije za upravljavcem.

Splošna uredba o varstvu podatkov zahteva, da upravljavec podatkov sodeluje samo s tistim obdelovalcem, ki ponuja zadostna jamstva. Ta jamstva morajo biti vključena v pisno pogodbo, ki jo skleneta upravljavec in obdelovalec podatkov. Pogodba mora vsebovati tudi številne obvezne klavzule, vključno s klavzulo, ki določa, da obdelovalec podatkov obdeluje osebne podatke samo v skladu z dokumentiranimi navodili upravljavca podatkov.

Obveznosti, ki ščitijo pravice posameznikov

Splošna uredba o varstvu podatkov vključuje številne obveznosti, katerih cilj je ščititi pravico posameznika do nadzora nad lastnimi osebnimi podatki.

Vaša obveznost: zagotoviti pregledne informacije

Podjetja morajo posameznikom zagotoviti informacije o tem, kdo obdeluje katere podatke in zakaj. V teh informacijah mora biti jasno navedeno vsaj naslednje:

- 👤 kdo ste,
- 👤 zakaj obdelujete podatke,
- 👤 kaj je pravna podlaga za to,
- 👤 kdo bo podatke prejel (če je relevantno).

V nekaterih primerih je treba navesti tudi:

- 👤 kontaktne informacije pooblaščenih oseb za varstvo podatkov,
- 👤 zakoniti interes (kadar je zakoniti interes pravna podlaga za obdelavo),
- 👤 podlago za prenos podatkov v državo zunaj EU,
- 👤 koliko časa se bodo podatki hranili,
- 👤 pravice posameznika glede varstva podatkov (tj. pravica dostopa, pravica do popravka, izbrisa, omejitve, ugovora, prenosljivosti itd.),
- 👤 kako se lahko privolitev prekliče (kadar je privolitev pravna podlaga za obdelavo),
- 👤 ali obstaja zakonska ali pogodbeno obveznost za zagotovitev podatkov,
- 👤 v primeru avtomatiziranega sprejemanja odločitev informacije o razlogih, pomenu in posledicah odločitve.

„Podjetja morajo posameznikom zagotoviti informacije o tem, kdo obdeluje katere podatke in zakaj.“

Vaša obveznost: pravica dostopa in pravica do prenosljivosti podatkov

Posamezniki imajo pravico zahtevati brezplačen dostop do svojih osebnih podatkov v dostopnem formatu. Če prejmete tak zahtevek, morate:

- ☝ posamezniku povedati, ali obdelujete njegove osebne podatke,
- ☝ ga obvestiti o obdelavi (npr. o namenih obdelave, kategorijah zadevnih osebnih podatkov, prejemnikih njihovih podatkov itd.),
- ☝ mu zagotoviti kopijo osebnih podatkov, ki jih obdelujete.

Kadar obdelava temelji na soglasju ali pogodbi, lahko posameznik zahteva tudi, da mu njegove osebne podatke vrnete ali jih prenesete na drugo podjetje. To je t. i. pravica do prenosljivosti podatkov. Podatke je treba zagotoviti v splošno uporabljani strojno berljivi obliki.

Čeprav sta ti pravici tesno povezani, gre za ločeni pravici. Zato morate zagotoviti, da se ne bosta zamenjevali, in o tem ustrezno obvestiti posameznike.

Vaša obveznost: pravica do izbrisa (pravica do pozabe)

V nekaterih primerih lahko posameznik od upravljavca podatkov zahteva, da njegove osebne podatke izbriše; npr. kadar podatki niso več potrebni za izpolnitev namena obdelave. Vendar vaše podjetje ni dolžno ugoditi taki zahtevi, če:

- ☝ je obdelava potrebna zaradi spoštovanja svobode izražanja in obveščanja posameznika,
- ☝ morate hraniti osebne podatke zaradi izpolnjevanja pravnih obveznosti,
- ☝ če za obdelavo osebnih podatkov obstajajo drugi razlogi javnega interesa, npr. zaradi javnega zdravja ali znanstveno- ali zgodovinskoraziskovalnih namenov,
- ☝ če morate osebne podatke hraniti zaradi pravnih zahtevkov.

Vaša obveznost: pravica do popravka in pravica do ugovora




Če posameznik meni, da so njegovi osebni podatki nepravilni, nepopolni ali netočni, ima pravico do njihovega popravka ali dopolnitve brez nepotrebnega odlašanja.

Posameznik lahko tudi kadar koli ugovarja obdelavi svojih osebnih podatkov za določene namene, kadar jih vaše podjetje obdeluje na podlagi vašega legitimnega

interesa ali za opravljanje naloge v javnem interesu. Če nimate zakonitega interesa, ki prevladuje nad interesom posameznika, morate obdelavo osebnih podatkov prekiniti. Posameznik lahko tudi zahteva, da se obdelava njegovih osebnih podatkov omeji, dokler se ne ugotovi, ali vaš zakoniti interes prevladuje nad njegovim interesom. V vsakem primeru pa ste dolžni prekiniti obdelavo osebnih podatkov, kadar se ti uporabljajo za neposredno trženje.

Opozorilo glede avtomatiziranega sprejemanja odločitev in oblikovanja profilov

Posamezniki imajo pravico, da zanje ne veljajo odločitve, ki temeljijo zgolj na avtomatizirani obdelavi. Vendar pri tem pravilu obstaja nekaj izjem: npr. kadar posameznik izrecno privoli v avtomatizirano sprejemanje odločitev. Če avtomatizirano sprejemanje odločitev ne temelji na zakonodaji, mora vaše podjetje:

-  obvestiti posameznika o avtomatiziranem sprejemanju odločitev,
-  zagotoviti mu pravico do pregleda avtomatizirane odločitve, ki ga opravi človek,
-  omogočiti mu, da ugovarja avtomatizirani odločitvi.

Če npr. banka sprejme avtomatizirano odločitev, da se posojilo nekomu odobri ali ne odobri, je treba tega posameznika obvestiti o avtomatizirani odločitvi in mu omogočiti, da taki odločitvi ugovarja in zahteva človekovo posredovanje.

Obveznosti na podlagi tveganja

Poleg obveznosti, katerih cilj je zaščititi posameznikove pravice, splošna uredba o varstvu podatkov vsebuje tudi številne druge obveznosti, katerih uporaba je odvisna od tveganja.

Vaša obveznost: imenovanje pooblaščenih oseb za varstvo podatkov

Pooblaščen osebja za varstvo podatkov je odgovorna za spremljanje vašega izpolnjevanja obveznosti iz splošne uredbe o varstvu podatkov. Ena od njenih osrednjih nalog je seznaniti zaposlene, ki izvajajo obdelavo osebnih podatkov, o njihovih obveznostih in jim v zvezi s tem svetovati. Pooblaščen osebja za varstvo podatkov sodeluje tudi z organom za varstvo podatkov in opravlja nalogo kontaktne točke za ta organ in posameznike.

Vaše podjetje mora imenovati pooblaščen osebja za varstvo podatkov, če:

- ☝ redno ali sistematično spremlja ali obdeluje posebne kategorije podatkov,
- ☝ je ta obdelava temeljna poslovna dejavnost in
- ☝ se izvaja v velikem obsegu.

Če npr. obdelujete osebne podatke, da bi na podlagi spletnega vedenja ljudi prek brskalnikov usmerjali oglasna sporočila, morate na podlagi splošne uredbe o varstvu podatkov imenovati pooblaščen osebja za varstvo podatkov. Če svojim strankam pošiljate promocijsko gradivo samo enkrat na leto, pa pooblaščen osebja za varstvo podatkov ne potrebujete. Če ste zdravnik, ki pridobiva podatke o zdravstvenem stanju pacientov, pooblaščen osebja verjetno prav tako ne boste potrebovali. Če obdelujete osebne podatke o genetiki in zdravstvenem stanju za bolnišnico, pa takšno osebja morate imenovati.

Vaša obveznost: vgrajeno in privzeto varstvo podatkov

Splošna uredba o varstvu podatkov uvaja novi načeli: vgrajeno in privzeto varstvo podatkov.

Vgrajeno varstvo podatkov pomaga zagotoviti, da podjetje upošteva varstvo podatkov že v zgodnji fazi načrtovanja novih načinov obdelave osebnih podatkov. V skladu s tem načelom mora upravljavec podatkov sprejeti vse potrebne tehnične in organizacijske ukrepe za izvajanje načel o varstvu podatkov in zaščito pravic posameznikov. Ti ukrepi bi npr. lahko vključevali psevdonimizacijo.

Z vgrajenim varstvom podatkov se zmanjša tveganje za zasebnost in povečuje zaupanje. Če se varstvo podatkov postavi v ospredje pri razvoju novega blaga ali storitev, se je problemom na tem področju mogoče ogniti že v zgodnji fazi. Ta praksa obenem pomaga ozaveščati o varstvu podatkov v vseh oddelkih in na vseh ravneh podjetja.

Privzeto varstvo podatkov pomeni zagotavljanje, da je delovna ureditev, ki najbolj spoštuje zasebnost, v vašem podjetju privzeta delovna ureditev. Če npr. obstaja možnost za dve obliki ureditve in ena od njiju onemogoča dostop do osebnih podatkov drugim osebam, se ta uporabi kot privzeta delovna ureditev.

„Z vgrajenim varstvom podatkov se zmanjša tveganje za zasebnost in povečuje zaupanje.“

„Privzeto varstvo podatkov pomeni zagotavljanje, da je delovna ureditev, ki najbolj spoštuje zasebnost, v vašem podjetju privzeta delovna ureditev.“

Vaša obveznost: ustrezno obveščanje ob kršitvi varstva osebnih podatkov

O kršitvi varstva osebnih podatkov govorimo ob naključnem ali nezakonitem razkritju osebnih podatkov, za katere ste odgovorni, nepooblaščenim prejemnikom ali kadar so podatki začasno nedostopni ali spremenjeni.

Za podjetje je bistveno, da izvaja ustrezne tehnične in organizacijske ukrepe za preprečevanje kršitev varstva podatkov. Če do kršitve podatkov vendarle pride in

če kršitev pomeni tveganje za pravice in svoboščine posameznika, mora o tem obvestiti organ za varstvo podatkov v 72 urah po seznanitvi s kršitvijo.

Če kršitev podatkov pomeni *veliko* tveganje za zadevne osebe, je od podjetja mogoče zahtevati tudi, da o tem obvesti vse posameznike, na katere kršitev podatkov vpliva.

Prenos osebnih podatkov zunaj EU

Splošna uredba o varstvu podatkov se uporablja za Evropski gospodarski prostor (EGP), ki vključuje vse države EU ter Islandijo, Lihtenštajn in Norveško. Kadar se osebni podatki prenašajo v države zunaj EGP, mora varstvo, ki ga zagotavlja splošna uredba o varstvu podatkov, potovati skupaj s podatki. To pomeni, da morajo podjetja, ki želijo izvažati podatke v tujino, zagotoviti izvajanje ustreznih zaščitnih ukrepov.

Splošna uredba o varstvu podatkov ponuja raznolik sklop orodij z mehanizmi za prenos podatkov v tretje države. V skladu s splošno uredb o varstvu podatkov so taki prenosi dovoljeni, kadar:

- 1.** varstvo, ki ga zagotavlja država, velja za skladno z zahtevami EU ali
- 2.** vaše podjetje npr. sprejme potrebne ukrepe za zagotovitev ustreznih zaščitnih ukrepov, tj. z vključitvijo posebnih klavzul v pogodbo, sklenjeno z uvoznikom osebnih podatkov zunaj Evrope, ali
- 3.** ima vaše podjetje npr. posebno podlago za prenos (t. i. „odstopanja“), kot je privolitev posameznika.

Za več informacij o predpisih, ki veljajo za mednarodne prenose podatkov, si preberite sporočilo Evropske komisije z naslovom „Izmenjava in varstvo osebnih podatkov v globaliziranem svetu“: <http://eur-lex.europa.eu/legal-content/SL/TXT/HTML/?uri=CELEX:52017DC0007&qid=1517491381997&from=SL>

Ali morate izvajati oceno učinka v zvezi z varstvom podatkov

Izvajanje ocene učinka v zvezi z varstvom podatkov je obvezno, kadar bi načrtovana obdelava lahko povzročila veliko tveganje za pravice in svoboščine posameznikov. To je npr. mogoče pri uporabi novih tehnologij.

V skladu s splošno uredbo o varstvu podatkov veliko tveganje obstaja že ob:

- 🔴 uporabi mehanizmov avtomatizirane obdelave in oblikovanja profilov za sistematično in obsežno ocenjevanje posameznikov,
- 🔴 sistematičnem nadzoru javno dostopnih območij v velikem obsegu (npr. z nadzornimi kamerami),
- 🔴 obdelavi občutljivih podatkov v velikem obsegu (npr. podatkov o zdravstvenem stanju).

Namen ocene učinka v zvezi z varstvom podatkov je opredeliti potencialna tveganja za pravice in svoboščine posameznikov še pred začetkom obdelave njihovih osebnih podatkov in preden se tveganje lahko uresniči. Z vnaprejšnjim zmanjševanjem tveganja je mogoče preprečiti škodo in zmanjšati stroške.

Če z ukrepom, navedenim v oceni učinka, ni mogoče odpraviti vseh prepoznanih velikih tveganj, se je treba pred načrtovano obdelavo podatkov posvetovati z organom za varstvo podatkov.

„Izvajanje ocene učinka v zvezi z varstvom podatkov je obvezno, kadar bi načrtovana obdelava lahko povzročila veliko tveganje za pravice in svoboščine posameznikov.“

Kaj morate storiti

Odgovori na zahteve

Če vaše podjetje prejme zahtevo posameznika, ki želi uveljaviti svoje pravice, morate nanjo odgovoriti brez nepotrebnega odlašanja, vsekakor pa v enem mesecu po prejemu zahtevka. Ob zapletenih ali številčnih zahtevah se rok za odgovor sicer lahko podaljša na dva meseca, a mora biti posameznik o tem podaljšanju obveščten. Poleg tega je treba zahteve obravnavati **brezplačno**. Če zahtevo zavrnete, morate posameznika obvestiti o razlogih za zavrnitev in ga seznaniti s pravico do pritožbe pri organu za varstvo podatkov.

Dokazovanje izpolnjevanja obveznosti in vodenje evidenc

Eno od glavnih načel, na katerih temelji splošna uredba o varstvu podatkov, je podjetjem zagotoviti možnost dokazati, da izpolnjujejo svoje obveznosti. To pomeni, da morate biti zmožni dokazati, da vaše podjetje deluje v skladu s splošno uredbo o varstvu podatkov in izpolnjuje vse veljavne obveznosti – zlasti na zahtevo organa za varstvo podatkov ali ob pregledih, ki jih ta organ izvaja.

To je npr. mogoče doseči z vodenjem podrobnih evidenc, kot so:

- 👤 ime in kontaktni podatki vašega podjetja, ki obdeluje podatke,
- 👤 razlogi za obdelavo osebnih podatkov,
- 👤 opis kategorij posameznikov, ki posredujejo osebne podatke,
- 👤 kategorije organizacij, ki prejemale osebne podatke,
- 👤 prenos osebnih podatkov v drugo državo ali organizacijo,
- 👤 obdobje hrambe osebnih podatkov,
- 👤 opis varnostnih ukrepov, ki se uporabljajo pri obdelavi osebnih podatkov.

Vaše podjetje mora hraniti in redno posodabljeni tudi pisne postopke in smernice ter z njimi seznanjati svoje zaposlene.



POGLAVJE 4

STE PRIPRAVLJENI IZPOLNITI OBVEZNOST?

Splošna uredba o varstvu podatkov določa, da ste, ko je treba zagotoviti varstvo podatkov, na potezi vi. Vaša prva naloga je opredeliti obstoječe dejavnosti obdelave podatkov in ponovno oceniti notranje poslovne procese. Predvsem morate:

- 🔥 opredeliti, katere podatke hranite in za kakšen namen ter na kakšni pravni podlagi,
- 🔥 oceniti vse sklenjene pogodbe, zlasti z upravljavci in obdelovalci,

- 🔥 oceniti vse razpoložljive poti za mednarodne prenose in
- 🔥 pregledati celotno upravljanje vašega podjetja (tj. katere informacijske in organizacijske ukrepe izvajate), vključno s tem, ali imate oziroma želite imenovati pooblaščenca za varstvo podatkov.

Bistveno v tem procesu je, da je v navedene preglede vključeno najvišje vodstvo vašega podjetja, zagotavljanje informacij in redno dopolnjevanje ter posvetovanje v zvezi s spremembami politike glede podatkov.

Obdelava podatkov v več državah

V primeru čezmejne obdelave je pristojni organ lahko nadzorni organ druge države in ne vaš nacionalni organ za varstvo podatkov. Navadno gre za organ za varstvo

podatkov države znotraj EU, v kateri je glavni sedež vašega podjetja (kjer se sprejemajo odločitve o načinih in namenu obdelave).

Tveganje neizpolnjevanja obveznosti

Ob neizpolnjevanju obveznosti iz splošne uredbe o varstvu podatkov se lahko predpišejo visoke globe, ki v nekaterih panogah dosegajo tudi do 20 milijonov EUR ali 4 % letnega prometa podjetja. Organ za varstvo podatkov lahko naloži dodatne popravljalne ukrepe, kot je odredba prenehanja obdelave osebnih podatkov. Ob tem ne pozabite, da neizpolnjevanje obveznosti lahko okrni tudi ugled.

Stroški neizpolnjevanja obveznosti iz splošne uredbe o varstvu podatkov daleč presegajo sredstva, vložena v uskladitev z uredbo.



Vprašanja? Pripombe?

Obrnite se na nacionalni organ za varstvo podatkov.

Poiščite svoj nacionalni organ za varstvo podatkov na spletu.

http://ec.europa.eu/justice/data-protection/article-29/structure/data-protection-authorities/index_en.htm

POMEMBNO OBVESTILO

Namen informacij in smernic v tej brošuri je prispevati k boljšemu razumevanju pravil EU o varstvu podatkov.

To je zgolj svetovalno orodje: pravno veljavnost ima samo besedilo splošne uredbe o varstvu podatkov. Samo ta uredba zato lahko vzpostavi pravice in obveznosti za posameznike. Tu predstavljene smernice ne ustvarjajo nobenih izvršljivih pravic ali pričakovanj.

Zavezujoča razlaga zakonodaje EU je v izključni pristojnosti Sodišča Evropske unije. Mnenja, izražena v teh smernicah, ne morejo vplivati na stališče, ki bi ga Komisija morda zastopala pred Sodiščem.

Niti Evropska komisija niti osebe, ki delujejo v njenem imenu, niso odgovorne za uporabo podatkov v tej brošuri.

Ta brošura odseva stanje v času njene priprave, zato bi se morala upoštevati kot „uporaben dokument“, odprt za izboljšave, njena vsebina pa se lahko spremeni brez predhodnega obvestila.

Stik z EU

Osebno

Po vsej Evropski uniji je na stotine informacijskih točk Europe Direct. Naslov najbližje lahko najdete na spletni strani: https://europa.eu/european-union/contact_sl.

Po telefonu ali elektronski pošti

Europe Direct je služba, ki odgovarja na vaša vprašanja o Evropski uniji. Nanjo se lahko obrnete:

- s klicem na brezplačno telefonsko številko: 00 800 6 7 8 9 10 11 (nekateri ponudniki lahko klic zaračunajo),
- s klicem na navadno telefonsko številko: +32 22999696 ali
- po elektronski pošti s spletne strani: https://europa.eu/european-union/contact_sl.

Iskanje informacij o EU

Na spletu

Informacije o Evropski uniji v vseh uradnih jezikih EU so na voljo na spletišču Europa: https://europa.eu/european-union/index_sl.

Publikacije EU

Brezplačne in plačljive publikacije EU lahko prenesete s spletišča EU Bookshop (<https://publications.europa.eu/bookshop>) ali jih na tem spletišču naročite. Za več izvodov brezplačnih publikacij se obrnite na Europe Direct ali najbližjo informacijsko točko (https://europa.eu/european-union/contact_sl).

Zakonodaja EU in drugi dokumenti

Do pravnih informacij EU, vključno z vso zakonodajo EU od leta 1952 v vseh uradnih jezikovnih različicah, lahko dostopate na spletišču EUR-Lex: <http://eur-lex.europa.eu>.

Odprti podatki EU

Do podatkovnih zbirk EU lahko dostopate na portalu odprtih podatkov EU (<http://data.europa.eu/euodp/sl>). Podatke lahko brezplačno prenesete in uporabite tudi v komercialne namene.

Splošna uredba o varstvu podatkov ureja način, kako podjetja obdelujejo osebne podatke in z njimi ravnajo. Če vaše podjetje ponuja blago in storitve kjer koli v EU, se bo po sprejetju enotnega evropskega zakona o varstvu osebnih podatkov moralo uskladiti predvsem z enim sklopom predpisov na tem področju.

Splošna uredba o varstvu podatkov poenostavlja zakonodajno okolje za podjetja in vam daje novo priložnost za izboljšanje upravljanja osebnih podatkov ter s tem povečanje zaupanja potrošnikov v vaše podjetje.

Ta brošura povzema obveznosti vašega podjetja, ki jih določa splošna uredba o varstvu podatkov.

europa.eu/dataprotection/sl

