GDPR priručnik

eventhorizon

Kako se pripremiti za primjenu GDPR-a

SADRŽAJ

UVOD

Što je GDPR?

GDPR ili General Data Protection Regulation je Opća uredba o zaštiti osobnih podataka, donešena od strane Europske unije 14. travnja 2016. Regulativa donosi okvir za postavljanje visokog standarda zaštite osobnih podataka svih građana EU.

Razlozi uvođenja, datum stupanja na snagu

Europska unija je donošenjem Opće uredbe o zaštiti podataka zadala snažan pravni okvir kojim će se ubuduće štititi korištenje svih osobnih podataka građana EU kao i građana zemalja nečlanica. Isto tako zadane su stroge mjere kažnjavanja koje stupaju na snagu odmah te je izričito naglašeno kako odstupanja, odgode i produžavanja prilagodbe neće biti.

Stoga proizlazi da je ključno za svaku organizaciju i tvrtku da se pripremi prema novim pravilima do roka kada Opća uredba stupa na snagu, s datumom **25. svibnja 2018. godine.**

Event Horizon pristup implementaciji

Od samih početaka razvijanja svojih produkata, Event Horizon polaže veliku pažnju u zaštitu svih podataka kojima klijent pristupa te ih obrađuje. To znači da su sve mjere enkripcije, tehničke mogućnosti korisničke autorizacije te same autentifikacije korisnika, postavljene na visoku razinu i uz najnovija tehnološka rješenja. To znači da su klijenti koji su kupovali Event Horizon sofverska rješenja i prije Opće uredbe, dobivali softversko rješenje koje je ispunjavalo 90% uvjeta koje danas GDPR uredba propisuje. Ostatak uvjeta usklađen je prema zadanim normama, sukladno koju Uredbi. Event Horizon je u suradnji s konzultantima i pravnim stručnjacima potpuno prilagodio svoja rješenja GDPR Uredbi.

Koga zahvaća Opća uredba o zaštiti podataka?

Sve tvrtke i organizacije koje sakupljaju osobne podatke svojih klijenata, partnera i zaposlenika. Ako nudite proizvode ili usluge untar Europske unije, uz to pratite i obrađujete osobne podatke klijenata, partnera i zaposlenika, trebate obratiti pažnju na GDPR. Ako ste izvan Europske unije a poslujete s članicom EU, također je potrebno planirati usklađivanje, kako bi postigli uvjete u kojima možete u budućnosti nastaviti poslovati ili sklapati nove poslove.

Kratko o GDPR-u.

GDPR ili General Data Protection Regulation je Opća uredba o zaštiti podataka, donešena od strane Europske unije 14. travnja 2016. Uredba donosi okvir za postavljanje visokog standarda zaštite osobnih podataka svih građana EU.

Uredba se sastoji od liste potrebnih sigurnosnih mjera i obvezi koje tvrtke i organizacije moraju ispuniti kako bi se ispunila zadana zaštita privatnosi osoba.

GDPR ulazi u punu primjenu nakon dvije godine priprema i prilagodbe u prijelaznom razdoblju, s datumom 25.05.2018., kada bi sve tvrtke trebale biti usklađene s Uredbom. Sve tvrtke i organizacije koje neće izvršiti uskladu, ulaze u rizik dobivanja visokih novčanih kazni te posljedica koje su negativne za tržišnu pozicju te odnose s partnerima i klijentima.

Samo za područje EU?

GDPR uredba bitna je i za organizacije i tvrtke izvan EU, jer sve se tvrtke koje posluju,ili žele poslovati s tvrtkama iz EU, moraju pridržavati istih pravila o zaštiti privatnosti svih osoba.

Koje su posljedice i kazne ako se ne uskladite s Uredbom?

Mjere propisane Uredbom imaju za zadaću zaštiti sve aktere koji su uključeni, te u konačnici izgraditi partnerstva s povjerenjem.

Tvrtke i organizacije koje se ne usklade s Uredbom, ulaze u rizik dobivanja visokih novčanih kazni koje su u rasponu do najviše 20 milijuna Eura ili 4 % godišnjih prihoda u cijelom svijetu, rizik od gubitka udjela na tržištu, gubitka partnerstva te nepovjerenje potencijalnih klijenata i kupaca.

KAKO PRISTUPITI IMPLEMENTACIJI

Event Horizon je u suradnji sa stručnjacima konzultantima razvio metodu implementacije koja se optimalno prilagođava svakom tipu organizacije. Osnovna pravila i smjernice za GDPR prilagodbu odose se na:

1. **Sigurno pohranjivanje osjetljivih podataka uz potpun raspon enkripcijskih metoda čiji zadatak je sprječavanje proboja, gubitka i krađe podataka.**

2. **Implementirati sigurne metode transfera, uporabe i pristupa osjetljivim podacima.**

3. **Monitoring korištenja i prijenosa osjetljivih podataka.**

4. **Automatizirano kriptiranje i postizanje zaštite podataka, kako bi se spriječio neautoriziran pristup ili gubitak podataka.**

5. **Osjetljivi podaci trebaju biti zaštićeni unutar granica svih država EU i izvan EU.**

6. **Osigurati kopije podataka na više razina kako bi se spriječio gubitak u slučajevima nepredvidivih okolnosti.**

7. **Ponuditi eksplicitnu privolu građana za obradu njihovih podataka i dati mogućnost odabira da se podaci potpuno izbrišu i zaborave.**

8. **Obrada podataka u skladu sa Uredbom te transparentnost svih procesa vezanih za postupanje s podacima.**

U nastavku ćemo dublje objasniti kako prethodno navedene smjernice mogu biti implementirane i koja se problematika pojavljuje kod pojedinih područja nužnih za usklađivanje prema GDPR-u.

KOJE SU KLJUČNE PROMJENE I ŠTO TVRTKE TREBAJU IMPLEMENTIRATI?

Imenovati službenika za zaštitu podataka

Obavezno imenovanje je u sljedećim slučajevima: javne službe, tvrtke koje obrađuju velike količine osobnih podataka (banke, osiguranja, i sl.) te tvrtke koje se primarno bave prikupljanjem i obradom podataka (agencije za istraživanje tržišta, marketinške tvrtke i sl.). Preporuča se ipak da svaka tvrtka imenuje vlastitog službenika. Osoba na toj poziciji zadužena je za monitoring, izvještaje te postizanje vjerodostojnosti procesa zaštite podataka. Također, mora implementirati tehničke i organizacijske mjere koje su u skladu s temeljnim načelima Opće uredbe o zaštiti podataka.

Osigurati okvir za zaštitu osobnih podataka

Tvrtke i organizacije biti će odgovorne za zaštitu i protok svih osjetljivih podataka koje prikupljaju. Podaci trebaju biti zaštićeni od trenutka prikupljanja do trenutka brisanja. Ovo je krucijalno za osjetljive osobne podatke kao što su podaci o zdravstvenom stanju, financijama te ostalim podacima koje svaka osoba kao građanin ima.

Sigurna pohrana podataka?

Podaci se pohranjuju na različite načine, od lokalne pohrane na raznim uređajima (usb, računala i sl.), do pohrane u oblaku tzv. „*Cloudu*", sve do klasične pohrane u fizičkoj ili tiskanoj formi. Tvrtke trebaju osigurati zaštitu podataka u svim oblicima pohrane. Tako se za pohranu na lokalnim uređajima mora osigurati enkripcija sa zaštitom putem lozinki. *Cloud* pohrana treba biti povjerena tvrtkama koje imaju iskustvo u pružanju ove usluge.

Računala koja su spojena na internet trebaju imati postavljene zaštite putem vatrozida, antivirusnih zaštiti te sigurnosnih lozinki.

Event Horizon kao tvrtka koja isporučuje softverska rješenja putem *Cloud-a*, surađuje sa najpozantijim data centrima i pružateljima *cloud* usluge.

Event Horizon pristup autentifikaciji korisnika omogućava više razine provjere identiteta, od klasične potvrde korisničkog imena i lozinke, do dodatnih mjera identifikacije putem sms-a, čitanja QR koda, provjere otiska prsta, provjere lica i slično.

Osigurati automatiziranu zaštitu podataka
Softversko rješenje treba biti dizajnirano tako da se samim procesom prikupljanja i obrade, čini i zaštita te enkripcija podataka. To znači da se odgovornost o samoj pohrani i dinamici prijenosa ne može prebaciti na osobe koje koriste sustav, jer time bi rizik od greške bio prevelik. Ljudski faktor činio bi okruženje koje je vrlo ranjivo na greške i propuste.
Arhitektura Event Horizon softverskih rješenja ispunjava zadane mjere automatizirane zaštite i enkripcije podataka.

Zadati procedure prilikom proboja podataka
Tvrtke i organizacije trebaju imati zadanu proceduru kojom se postupa prilikom mogućeg proboja podataka ili uslijed nastanka događaja koji se ocijeni rizičnim. Općom uredbom propisane su mjere kojima se zadaju koraci ako se unatoč svim zadanim pravilima, podaci pojave u nesigurnoj situaciji. U tom trenutku tvrtke ili organizacije moraju regirati odmah u oajavještavanju subjekata, bez odgode. Svako prikrivanje ili odgoda biti će kažnjavane.

Prikupljanje podataka uz privolu
Svi podaci koji se prikupljaju trebaju biti pod privolom, odnosno svaki subjekt treba eksplicitno odobriti da se njegovi podaci mogu pohraniti i koristiti u jasno zadanu svrhu.

Protok podataka u državama koje su izvan EU

Nova GDPR uredba omogućava slobodan protok podataka kroz sve države izvan EU, međutim potrebno je da svi subjekti koji sudjeluju u procesu razmjene podataka, imaju regulirane iste mjere o zaštiti osobnih podataka.

Tvrtke ovdje moraju pripaziti da se to odnosi ne samo na njihove partnere i klijente izvan EU s kojima surađuju, već da se to odnosi i na pružatelje *Cloud* usluga koji su izvan EU, a koji trebaju imati ispunjene sve zahtjeve za zaštitom podataka sukladno GDPR Uredbi.

Omogućiti jasan i precizan pristanak na prikupljanje i profiliranje podatka te zadavanje prava na brisanje i zaborav

Prikupljanje podataka mora jasno biti definirano kao postupak koji je pod punim pristankom osobe čiji podaci se prikupljaju. Također mora biti jasno definirano zbog kojeg razloga se podaci prikupljaju i kako će se obrađivti.

Organizacije i tvrtke moraju dati subjektima čiji se podaci koriste jednostavnu mogućnost isključivanja (tzv. *"Opt-out"*) njihovih osobnih podataka iz baze, odnosno brisanja te zaborava.

Pseudonimizacija - mogućnost anonimne identifikacije
Sukladnom novom GDPR-u, tvrtke i organizacije trebaju dati mogućnost pseudonimizacije, odnosno obradu osobnih podataka na način da se osobni podaci više ne mogu pripisati određenom ispitaniku.

Kodeksi ponašanja koji omogućavaju demonstraciju o sukladnosti s GDPR-om.
Potiče se da svaka organizacija i tvrtka na izradu kodeksâ ponašanja kojim se regulira i održava primjena GDPR uredbe.

KAKO EVENT HORIZON MOŽE OLAKŠATI VAŠU GDPR PRILAGODBU?

Od samih početaka razvijanja svojih produkata, Event Horizon polaže veliku pažnju u zaštitu svih podataka kojima klijent pristupa. To znači da su sve mjere enkripcije i tehničke mogućnosti korisničke autorizacije te same autentifikacije korisnika, postavljene na visoku razinu uz najnovija tehnološka rješenja. Event Horizon softverska rješenja prilagođena su sukladno Uredbi.

Osim tehničke prilagodbe, Event Horizon će uskladiti vaše interne organizacijske i procesne postavke, kako bi se potpuno uskladili s novom Uredbom. Proces se sastoji od četiri faze:

Procjena

Analiza trenutnog stanja Dosadašnji način prikupljanja i obrade podataka, mjere sigurnosti i enkripcije podataka. Pristup podacima i mapiranje podataka.

Planiranje

Izrada strategije implementacije. Izrada plana nadogradnje ili promjene sustava u dijelovima obrade podataka, zaštite i čuvanja podataka.

Implementacija

Izrada dokumentacije i implementacija alata za provođenje Uredbe. Nadogradnja IT sustava potrebnim sigurnosnim alatima, zadavanje procesnih tijekova.

Revizija

Pregled svih faza implementacije i testiranje o usklađenosti sa Uredbom. Testiranje tehničkih alata te internih procesnih radnji. Izvještaj o implementaciji.

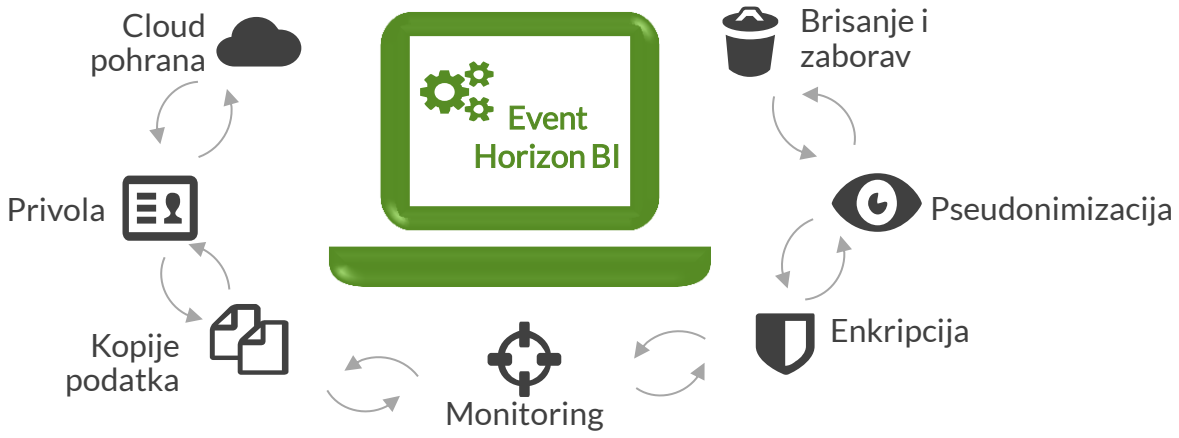
EVENT HORIZON produkti | GDPR usklađenost

Event Horizon BI

Business Inteligence softverski paket

Predstavlja višemodulari i sveobuhvati softverski paket koji objedinjuje sve segmente poslovanja organizacija i tvrtki, od malih poduzetnika do velikih tvrtki.

Potpuna tehnička podrška najsuvremenijih alata i servisa koji omogućavaju GDPR primjenu. Event Horizon isporučuje svoja rješenja na načine koji ispunjavaju GDPR zahtjeve:



Event Horizon isporučuje svoja rješenja prema GDPR zahtjevima:

- Cloud pohrana podataka u najpoznatijim data centrima s GDPR usklađenim mjerama - sigurno *Cloud* poslovanje
- Suvremene metode enkripcije podataka uz mogućnost više razina provjere identiteta korisnika
- Data mirroring - sigurnosne kopije podataka na više razina
  - sinkronizacija i kopiranje na više instanci
- Sigurnosni certifikati i protokoli koji štite protok podataka
  - https i ostali certifikati
- Automatizirana pohrana novo nastalih podataka
  - sinkronizacija na svim uređajima - mobitel, tablet, web
- Zadavanje opcije privole na razumljiv i praktičan način za korisnika
- Automatske izvještajne forme i zahtjevi prema zadanim GDPR mjerama

Izvještaji o korištenju sustava na zahtjev
- izvještaj o prikupljenim podacima i načinu prikupljanja podataka
- izvještaj o traženom brisanju podataka
- izvještaj o zaboravu
- zahtjev za brisanjem i zaboravom podataka

Automatsko alarmiranje kod potencijalnih opasnosti za podatke
- trenutno slanje email-a tvrtki ili organizaciji
- generiranje email poruke korisniku prema zadanom okviru od 72 sata

Jednostavan način ispunjavanja zahtjeva za brisanjem i zaboravom podataka po zahtjevu korisnika

Mogućnost opcije pseudonimizacije - anonimna identifikacija

Stalni monitoring sustava i alati za detekciju potencijalnih opasnosti od proboja podataka

Kome je Event Horizon BI prilagodljiv za implementaciju prema GDPR-u

OBRTINICI I SAMOSTALNE DJELATNOSTI

Mali obrtnici koji imaju podatke o klijentima, partnerima i zaposlenicima. Putničke agencije, medicinske usluge – stomatolozi, agencije za nekretnine, razne uslužne djelatnosti, odvjetnički uredi.

MALI PODUZETNICI

Poduzetnici koji se bave raznim proizvođačkim i uslužnim djelatnostima – imaju podatke o klijentima, partnerima, prikupljene kroz poslovanje ili marketinške aktivnosti.

VELIKE TVRTKE

Veće tvrtke koje pohranjuju podatke o svojim zaposlenicima parterima, klijentima.

VELIKE KORPORACIJE – ORGANIZACIJE, INSTITUCIJE, UDRUGE

Napomena: Ovaj dokument služi isključivo za opću informiranost o GDPR-u i ne predstavlja tumačenje Uredbe."

KONTAKT

Savska cesta 41
10000 Zagreb

+385 (0)1 58 11 296

info@event-horizon.hr

www.event-horizon.hr