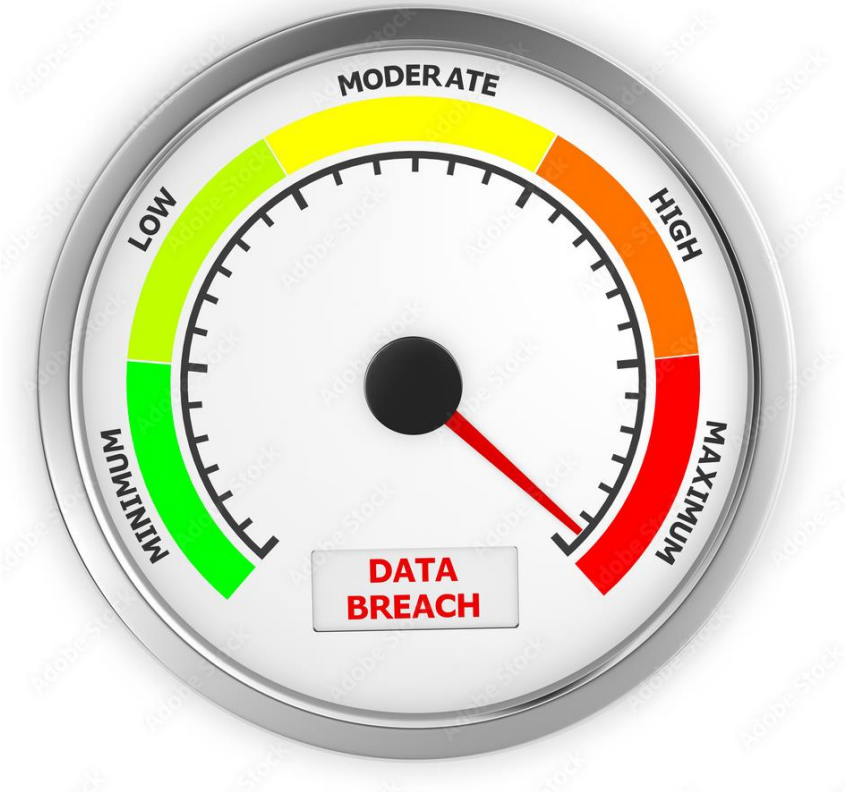


GDPR: VODIČ ZA TVRTKE PRILIKOM NADZORA ZBOG KRŠENJA GDPR

FERALIS PRIVACY CENTER

Vodič sadrži kriterije i korake kod utvrđivanja kršenja GDPR prilikom nadzora i primjerenu korektivnih mjera i upravnih novčanih kazni za tvrtke.
Izvor: Radna skupina za zaštitu podataka iz članka 29 - "Smjernice o primjeni i određivanju upravnih novčanih kazni za potrebe Uredbe 2016/679"- wp 253

Autori: Ines & Marko Krečak

Kriteriji u određivanju korektivnih mjera i upravnih novčanih kazni kod kršenja GDPR

Iako novčano kažnjavanje nije nikada svrha samo sebi, u prirodi pojedinca je sposobnost mijenjanja razmišljanja I navika kada se za određenu zakonsku normu propišu visoke novčane kazne. Ponegdje se takav zaokret dogodi trenutno ne provjeravajući snagu i učinkovitost provedbe na vlastitoj koži, ali statistički uvijek postoji određeni broj onih koji u potpunosti ne shvate svrhu i značaj visokog kažnjavanja, te se u različitoj mjeri ne pridržavaju zakona.

U poslovanju vrijedi slično pravilo koje kaže da se snaga regulatorne norme mjeri visinom novčane kazne. Unatoč suviše reguliranom tržištu, poduzetnici uz pomoć stručnih osoba pronalaze načine kako poslovati u okvirima zakona. Zakonske norme su, unatoč svojoj nepopularnosti, po prirodi okvir koji su poslodavci dužni poštovati s

manjim utjecajem na suštinski dizajn poslovanja, pa su formati, metode I rokovi za poštivanje jasni i jednoobrazni, a novčane kazne ili rasponi su dovoljno egzaktni da poduzetnici imaju konkretnu sliku rizika za svoje poslovanje.

GDPR I POSLOVNI SUBJEKTI

Kada govorimo o primjeni Opće uredbe (GDPR) u poslovanju, situacija može izgledati drugačije. U prvom redu, Opća uredba je krovni okvir Europske unije kojemu se prilagođavaju svi drugi zakoni Unije, ali i nacionalna zakonodavstva u pogledu zaštite osobnih podataka. Pored novih obveza za subjekte (poput ostvarivanja prava za pojedince, formiranja evidencija aktivnosti obrade i upravljanja povredama) u osnovi regulira što sve može biti osobni podatak, kako se prikuplja, obrađuje, razmjenjuje i pohranjuje propisujući mjere zaštite i sigurnosti u obradi. To znači da ima direktni utjecaj na kreiranje i promjene kod partnerskih odnosa, radnih odnosa, poslovnih procesa, pravila pristupa osobnim podacima te IT sustava za razmjenu i pohranu podataka. Kako se svi segmenti poslovanja neprestano unaprjeđuju, promjenom postojećih ili stvaranjem novih, poslovanje je glavni okidač trajne prisutnosti GDPR u samom kreiranju poslovanja.

Unatoč određenim prednostima u poslovanju, većina subjekata je prilagodila svoje poslovanje Općoj uredbi radi zakonitosti poslovanja i samog izbjegavanja novčanih kazni. A kada govorimo o novčanim kaznama, treba naglasiti da ne postoje jasno definirani iznos ili raspon. Međutim, postoje *Smjernice o primjeni i određivanju upravnih novčanih kazni za potrebe Uredbe 2016/679* koje govore što sve nadzorno tijelo ima na raspolaganju I kako može procjenjivati prilikom određivanja odgovarajuće korektivne mjere.

Nakon što se utvrdi da je došlo do kršenja Uredbe, nadzorno tijelo određuje najprikladnije korektivne mjere čije je izricanje učinkovito, proporcionalno i odvraćajuće kako bi se opet poštovala Uredba ili kaznilo nezakonito ponašanje a moguće i oboje.

PROCJENA KRŠENJA

Prilikom procjene, uzimaju se u obzir priroda, težina i trajanje kršenja. Pokazatelj težine kršenja može biti ne samo priroda kršenja, već i opseg, svrha predmetne obrade kao i broj pojedinaca i razina štete koju su pretrpjeli. Broj pojedinaca bi se trebao gledati proporcionalno (npr. od ukupnog broja korisnika), a ukoliko je pretrpljena šteta zbog kršenja Uredbe, tada bi se to trebalo uzeti u obzir pri odabiru korektivne mjere bez obzira što nadzorno tijelo ne određuje naknade za pretrpljenu štetu.

Jedan od kriterija prilikom procjenjivanja kršenja je i da li je nastala namjerom ili nepažnjom. Okolnosti koje su znak namjernih kršenja mogu uključivati nezakonitu obradu koju je izričito naložila uprava voditelja obrade ili onu koja se obavlja suprotno savjetu službenika za zaštitu podataka, ili koja se obavlja zanemarujući postojeće propisane mjere. S druge strane, okolnosti nepažnje su primjerice ljudska pogreška, nepravovremena primjena tehničkih ažuriranja i slično. Iako će ponekad biti teško razaznati namjeru od nepažnje, to ne znači da će se kao opravdanje moći upotrijebiti razlog da subjekt nije imao dovoljno resursa za provođenje Uredbe i sprječavanje kršenja.

Nadzorno tijelo će procijeniti je li ponašanje subjekta bilo odgovorno ili ne prilikom odabira korektivnih mjera te tijekom izračuna visine sankcije koja će se izreći u određenom slučaju, pa je dobro spomenuti kako otegotne i olakotne okolnosti mogu igrati važnu ulogu u odabiru odgovarajuće korektivne mjere. Naime, Nadzorno tijelo nakon procjene se može naći u situaciji da nije sigurno treba li upravnu novčanu kaznu odrediti kao samostalnu korektivnu mjeru ili u kombinaciji s ostalim mjerama iz članka 58. Zbog toga je važno da kada dođe do kršenja i ispitanik pretrpi štetu, subjekt učini sve što je u svojoj moći da ublaži posljedice koje bi kršenje moglo imati na predmetne pojedince. Primjeri takvog pozitivnog ponašanja iz regulatorne prakse može biti kontaktiranje trećih strana koji su možda sudjelovali u daljnjoj obradi ili pravodobno djelovanje subjekta kako bi se spriječilo daljnje kršenje po kojoj bi posljedice bile daleko ozbiljnije.

PROCJENA STUPNJA ODGOVORNOSTI

Pri određivanju stupnja odgovornosti subjekta može se voditi računa o sljedećim pitanjima:

- Je li subjekt proveo tehničke i organizacijske mjere u skladu s načelima tehničke ili integrirane zaštite podataka kao i mjere za postizanje primjerene razine sigurnosti
- Jesu li svi odgovorni upoznati s rutinskim postupcima zaštite podataka / politikama i primjenjuju li se oni na odgovarajućoj rukovodećoj razini u organizaciji?

Pri tome subjekti su dužni uzeti u obzir najnovija dostignuća, trošak provedbe te prirodu, opseg, kontekst i svrhe obrade, kao i rizike različitih razina vjerojatnosti i ozbiljnosti za prava i slobode pojedinaca koji proizlaze iz obrade podataka. Na osnovi toga nadzorno tijelo procjenjuje u kojoj je mjeri voditelj obrade napravio sve što je bilo u njegovoj mogućnosti. Tijekom te procjene trebali bi se uzeti u obzir standardi poslovanja i kodeksi ponašanja u odgovarajućem sektoru ili struci, iz kojih se može naslutiti koja je uobičajena praksa kao i koja je razina znanja o načinima rješavanja karakterističnih sigurnosnih situacija.

Treba napomenuti da i sva prijašnja kršenja, bez obzira na prirodu utječu na procjenu konkretne situacije, jer mogu osnovano upućivati na općenito nepoznavanje razumijevanja i primjene Uredbe u poslovanju.

PROCJENA STUPNJA SURADNJE

Premda Uredba ne daje konkretan odgovor na pitanje kako treba vrednovati stupanj suradnje prilikom određivanja korektivne mjere, ako su postupci subjekta ograničili ili u potpunosti poništili negativni utjecaj takvo djelovanje bi se moglo uzeti u razmatranje pri odabiru korektivne mjere.

Primjer takve suradnje bi mogli biti učinkoviti odgovori subjekta na zahtjeve nadzornog tijela tijekom inspekcijskog nadzora, a koji su doveli do smanjenja negativnog utjecaja na prava pojedinaca.

KATEGORIJE PODATAKA I SURADNJA S NADZORNIM TIJELOM

Kada govorimo o samim osobnim podacima koji su predmet kršenja, nadzorno tijelo će svakako pokušati utvrditi odnosi li se kršenje na obradu posebnih kategorija podataka, mogu li se isti povezati direktno s pojedincima, da li su kršenjem neposredno ugrožena prava pojedinaca te da li su podaci bili s odgovarajućom tehničkom zaštitom kriptirani ili ne.

Kada voditelj obrade ustanovi da je došlo do kršenja, neovisno o razini saznanja o samom kršenju bez odgađanja je obvezan obavijestiti nadzorno tijelo. Otegotna okolnost bi se uzelo ako je nadzorno tijelo saznalo o kršenju od trećih strana (npr. iz medija, anonimnom dojavom i sl). Ali, ako je voditelj obrade obavijestio s odgađanjem od trenutka saznanja ili nije naveo sva saznanja se također može uzeti kao otegotna okolnost.

OSTALI ELEMENTI

Od ostalih elemenata koji bi se mogli uzeti u obzir kada se odlučuje je li primjereno izreći upravnu novčanu kaznu za kršenje odredbi, ostvarena financijska dobit ili druga vrsta tržišne prednosti koja je ostvarena kršenjem može upućivati na odluku o izricanju upravne novčane kazne.

ZAKLJUČAK

Proces izricanja korektivnih mjera i upravnih novčanih kazni je dugotrajan i neprekidno se usavršava na razini Europske Unije. Kršenje Uredbe se u dinamici poslovanja može makar i nenamjerno dogoditi i subjektima s najvišom razinom usklađenosti i održavanja iste. No, kad se i dogodi, znatno širi spektar elemenata se uzima prilikom procjene. Zbog toga su prilagodba poslovanja, konkretno provođenje unutar organizacije i kontinuirano preispitivanje usklađenosti sa Uredbom najbolje i jedino isplativo rješenje da čak i kada se dogode kršenja postoje mehanizmi i argumentacija kojom će nadzorno tijelo izreći učinkovitu, proporcionalnu i odvraćajuću korektivnu mjeru koja će i kao takva imati najmanji mogući negativni učinak na poslovanje organizacije.

PRILOG 01: Obrazac Izvješća o povredi osobnih podataka (Izvor: Agencija za zaštitu osobnih podataka)

IZVJEŠĆE

o povredi osobnih podataka

temeljem članka 33. UREDBE (EU) 2016/679 EUROPSKOG PARLAMENTA I VIJEĆA od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka)

* Voditelj obrade:

_____

(navesti registrirani službeni naziv Voditelja obrade)

* Sjedište Voditelja obrade:

_____

(navesti adresu, poštanski broj i mjesto sjedišta Voditelja obrade)

* OIB Voditelja obrade:

_____

(navesti OIB Voditelja obrade)

* Službenik za zaštitu podataka (ili druga kontakt osoba):

_____

(navesti ime i prezime, adresu rada službenika za zaštitu podataka, te navesti svojstvo – ukoliko se funkcija obavlja temeljem ugovora o djelu, broj telefona za kontakt i e-mail adresu za kontakt službenika za zaštitu podataka ili druge kontakt osobe)

* Opis prirode povrede osobnih podataka:

_____

_____

_____

_____

(uključujući procijenjeno vrijeme nastupa povrede, kategorije i približan broj ispitanika na koje se povreda odnosi te kategorije i približan broj evidencija osobnih podataka na koje se povreda odnosi)

* Vrijeme saznanja o povredi osobnih podataka:

_____

(uključujući razloge kašnjenja ukoliko izvješćivanje nije učinjeno unutar 72 sata od saznanja o povredi osobnih podataka)

* Vjerojatne posljedice povrede osobnih podataka:

* Mjere koje je voditelj obrade poduzeo ili predložio poduzeti za rješavanje problema povrede osobnih podataka:

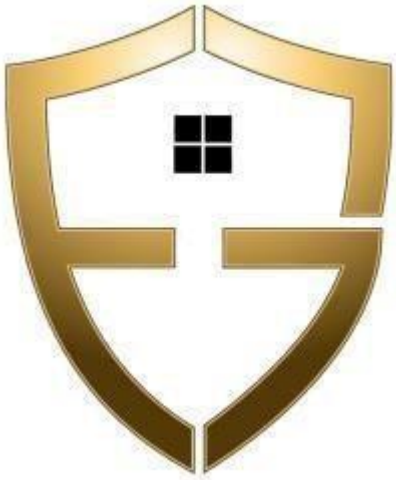
(uključujući prema potrebi mjere umanjivanja mogućih štetnih posljedica predmetne povrede)

Mjesto: Dana:

* M.P. *

(Klasa, Urbroj i ostali neobvezni podaci) (pečat Voditelja obrade – ako je primjenjivo) (potpis odgovorne osobe kod Voditelja obrade)

(Potrebno je u obrascu popuniti sve obvezne podatke (označeni su zvjezdicom) i izvješće s potpisom odgovorne osobe i pečatom (ako je primjenjivo) Voditelja obrade, u izvorniku, dostaviti na adresu sjedišta Agencije:
Agencija za zaštitu osobnih podataka**, Selska cesta 136, 10000 Zagreb**, te skenirano na e-mail adresu: **incidenti@azop.hr)**



EUROPEAN FEDERATION
OF DATA PROTECTION OFFICERS

Centar Feralis predstavnik je HR u Europskoj federaciji službenika za zaštitu podataka

INFO
Feralis Privacy Center
OIB 12963506386
IBAN HR3024020061101030774

ADRESA
Jože Gabrovšeka 8
Rijeka 51000
Hrvatska

KONTAKT
feralis@feralis.hr
+385 91 7881 535
+385 99 563 9746

WEB
www.feralis.hr
FB @feralis.hr
Inst. feralis.centar

Društvo je upisano u sudski registar Trgovačkog suda u Rijeci pod brojem MBS 040427386, osobni identifikacijski broje (OIB): 12963506386, europski jedinstvenim identifikator (EUID): HRSR.040427386. Temeljni kapital društva 20.000,00 kn. Predsjednik uprave: Marko Krečak. Direktor društva: Ines Krečak. Račun za redovno poslovanje društva vodi se kod Erste & steiermärkische bank d.d IBAN: HR3024020061101030774