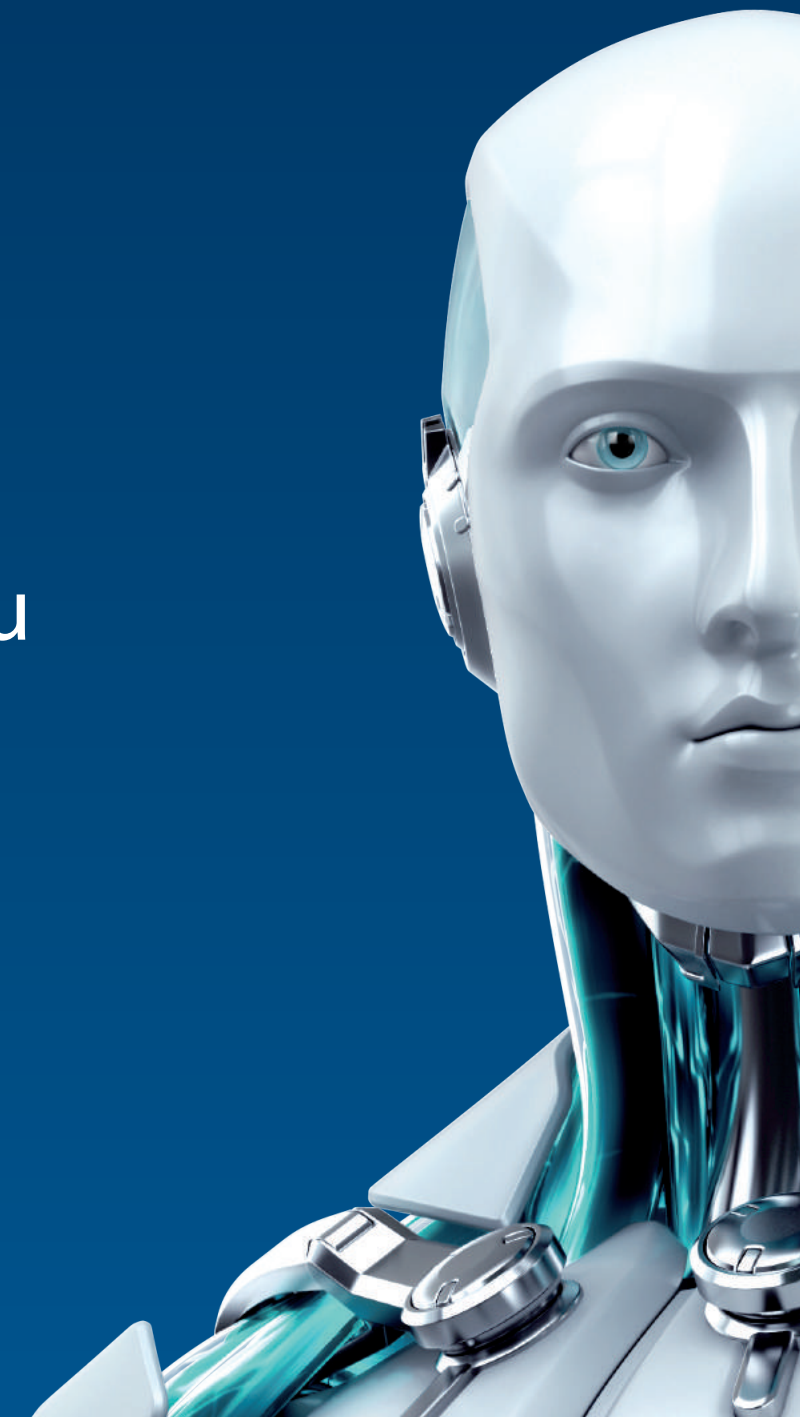
DESLOCK
ENCRYPTION BY

ESET

Vodič za EU regulativu u području zaštite podataka - General Data Protection Regulation



ENJOY SAFER TECHNOLOGY™

NOVA REGULATIVA ZA ZAŠTITU OSOBNIH PODATAKA

Nedavno usvojena regulativa Europske unije pod nazivom General Data Protection Regulation (GDPR) od sljedeće godine zamjenjuje direktivu Data Protection Directive 95/46/EC Europske unije iz 1995. godine. GDPR regulativa je razvijena s ciljem osnaživanja i usklađivanja prava na privatnost i zaštitu osobnih podataka na Internetu unutar Europske unije te obaveza zaštite podataka za poduzeća koja posluju s građanima Europske unije putem jedinstvene regulative koja zamijenjuje 28 zasebnih nacionalnih zakona.

Europska komisija je 8. travnja 2016. godine usvojila GDPR, a 14 travnja je regulativa usvojena i u Europskom parlamentu. Službeni tekst regulative je objavljen u službenom glasilu Europske unije 4. svibnja 2016. godine, a regulativa stupa na snagu 28. svibnja 2018. godine.

28 zemalja članica je u različitoj mjeri usvojilo pravila iz 1995. godine, što je dovelo do poteškoća i troškova za poduzeća koja posluju na više tržišta u Europskoj uniji s velikim razlikama u primjeni zaštite podataka. Procjenjuje se da će uklanjanje ove razdrobljenosti dovesti do ušteda za takva poduzeća u ukupnom iznosu od oko 2,3 milijarde eura godišnje.

U ČEMU SE SASTOJE IZMJENE?

Ključne izmjene koje stupaju na snagu s uvođenjem GDPR regulative se sastoje u sljedećem[1]:

- Pravo na obavijest u slučaju neovlaštenog pristupa osobnim podacima: poduzeća i institucije moraju obavijestiti nacionalno nadzorno tijelo o neovlaštenim pristupima osobnim podacima koji mogu ugroziti privatnost pojedinaca te obavijestiti vlasnika podataka o svim povredama sigurnosti podataka kako bi mogli poduzeti odgovarajuće mjere.

- Stroža primjena pravila: državna tijela ovlaštena za zaštitu podataka će imati ovlasti za izricanje kazni poduzećima čije poslovanje nije usklađeno s GDPR regulativom do visine od 4% njihovih globalnih prihoda. Visina administrativne kazne nije propisana zakonom te se o njoj odlučuje zasebno u svakom slučaju. Kazne moraju biti efikasne, proporcionalne težini prekršaja te imati preventivni efekt.

- Jedan kontinent, jedan zakon: jedinstveni europski zakon za zaštitu podataka mijenja postojeće zasebne nacionalne zakone. Poduzeća se usklađuju s jednim zakonom umjesto s 28 različitih regulativa. Uštede za poduzeća se procjenjuju na otprilike 2,3 milijarde eura godišnje.

- Organizacije moraju obavijestiti nadležna državna tijela o ozbiljnoj povredi sigurnosti podataka u najkraćem mogućem roku (unutar 24 sata, ukoliko je to moguće).

- Pravila Europske unije se primjenjuju i u slučajevima kada kompanije koje su aktivne na europskom tržištu te prodaju svoje proizvode i usluge ili prate ponašanje pojedinaca u Europskoj uniji obrađuju podatke izvan granica Europske unije.

- Uzimanje zaštite podataka u obzir prilikom dizajna: 'zaštita podataka u dizajnu' te 'standardna zaštita podataka' sada predstavljaju osnovne principe zaštite podataka u Europskoj uniji. Mehanizmi za zaštitu podataka moraju biti ugrađeni u proizvode i usluge u najranijoj fazi razvoja, a zaštita podataka se iz dobre poslovne prakse pretvara u standard.

Osnaživanjem regulative za zaštitu podataka, Europska unija obavezuje poduzeća i institucije da na odgovarajući način zaštite osjetljive privatne podatke, na primjer:

"...bilo koje podatke koji se odnose na određenu ili odredivu privatnu osobu, u daljnjem tekstu 'vlasnika podataka'; odrediva osoba je osoba koju je moguće identificirati, direktno ili indirektno, prema nekom identifikacijskom broju ili jednom ili više faktora tipičnih za njen fizički, fiziološki, mentalni, ekonomski, kulturni ili socijalni identitet;"[2]

Ova široka definicija osobnih podataka pokriva i najjednostavnije zapise koji se makar indirektno odnose na kupce, klijente, osoblje, učenike ili bilo koje druge podatke koji se odnose na privatne osobe.

1 Sažetak objave za medije: http://europa.eu/rapid/press-release_MEMO-15-6385_en.htm

2 REGULATION (EC) No 45/2001:

http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1484915514779&uri=CELEX:32001R0045

ŠTO REGULATIVA GOVORI O ZAŠTITI PODATAKA?

Članak 32. o sigurnosti obrade podataka kaže[3]:

1. Uzimajući u obzir stupanj razvoja, troškove uvođenja i prirodu, opseg, kontekst i namjenu obrade podataka, kao i rizike razne razine i vjerojatnosti za prava i slobode privatnih osoba, kontrolor i procesor će uvesti odgovarajuće tehničke i organizacijske mjere kako bi osigurali razinu sigurnosti koja odgovara riziku, uključujući između ostalog i sljedeće mjere:

a) Unošenje pseudo-podataka i enkripciju osobnih podataka;

b) Osiguravanje stalne povjerljivosti, integriteta, dostupnosti i stabilnosti sustava i servisa koji obavljaju obradu podataka;

c) Mogućnost brzog uspostavljanja ponovne dostupnosti i pristupa osobnim podacima u slučaju fizičkog ili tehničkog incidenta;

d) Plan redovitog testiranja, ocjenjivanja i procjene efikasnosti tehničkih i organizacijskih mjera za sigurnost obrade.

Enkripcija predstavlja najjednostavniji i najefikasniji način osiguravanja podataka u skladu sa zahtjevima Članka 32. GDPR regulative. Ova tehnologija je široko rasprostranjeni način zaštite informacija koje su izložene riziku od krađe ili gubitka. GDPR regulativa također zahtijeva postojanje efikasnog plana povrata podataka i lozinki te ključnih sistema za upravljanje u slučaju incidenta.

Članak 30. regulative zahtjeva postojanje pismene evidencije, zajedno s opisom poduzetih tehničkih i organizacijskih mjera, u skladu s Člankom 32, što znači da institucije moraju biti u stanju dokazati da su sistemi sigurni te da se šifrirani podaci mogu vratiti u slučaju tehničkog incidenta.

KOJE SU OBAVEZE OBAVJEŠTAVANJA U SLUČAJU POVREDE SIGURNOSTI PODATAKA?

Članak 33. zahtijeva da se o slučaju povrede sigurnosti osobnih podataka obavijesti nadzorno državno tijelo u roku od 72 sata od trenutka kada je institucija saznala za incident.

Obavijesti izdane nakon isteka ovog roka moraju biti popraćene opravdanjem kašnjenja.

Članak 34.[3] regulira obavještavanje vlasnika podataka o povredi sigurnosti podataka te kaže sljedeće:

> *1. U slučaju kada povreda sigurnosti podataka može dovesti do ugrožavanja prava i sloboda privatnih osoba, kontrolor će bez odlaganja obavijestiti vlasnika podataka o incidentu.*

Međutim, regulativa u nastavku kaže:

3. Obavještavanje vlasnika podataka u skladu s paragrafom 1 neće biti potrebno ukoliko je ispunjen bilo koji od sljedećih uvjeta:

a) Kontrolor je uveo odgovarajuće tehničke i organizacijske mjere zaštite i te mjere su primjenjene na osobne podatke čija sigurnost je narušena, a posebno kada se radi o mjerama kao što je enkripcija, koje čine osobne podatke nečitljive bilo kojoj neovlaštenoj osobi;

b) Kontrolor je poduzeo naknadne mjere koje osiguravaju da se rizici za prava i slobode vlasnika podataka navedeni u paragrafu 1 više neće pojaviti;

c) Obavještavanje vlasnika podataka bi zahtijevalo neproporcionalne napore. U takvom slučaju će se za obavještavanje koristiti javna komunikacija ili slična mjera kojom će vlasnici podataka biti obaviješteni na jednako efikasan način.

Studije pokazuju kako svako odgađanje obavještavanja o povredi sigurnosti podataka povećava štetu za organizaciju u kojoj se dogodio incident. Vidljivo je kako enkripcija predstavlja dovoljnu zaštitu od ovog rizika i posljedica za reputaciju poduzeća.

3 Tekst regulative se nalazi na:

http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN

NA KOJI NAČIN REGULATIVA OBESHRABRUJE IZBJEGAVANJE ZAŠTITE PODATAKA?

O kaznama za prekršaj odredbi GDPR regulative govori 4. stavak Članka 83. o općim uvjetima prekršajnih kazni:

4. Prekršaj sljedećih odredbi će u skladu s paragrafom 2 biti podložan administrativnoj kazni u iznosu do 10.000.000,00 eura ili, ukoliko je taj iznos veći, do 2% ukupnih globalnih prihoda u protekloj financijskoj godini u slučaju kada se radi o poduzeću:

a) Obaveze kontrolora i procesora prema Člancima 8, 11, 25-39, 42. i 43, koji predstavljaju pravila obavještavanja o povredi sigurnosti

Članak 33. i Članak 34. te 5. stavak Članka 83. navode:

5. Prekršaj sljedećih odredbi će u skladu s paragrafom 2 biti podložan administrativnoj kazni u iznosu do 10.000.000,00 eura ili, ukoliko je taj iznos veći, do 2% ukupnih globalnih prihoda u protekloj financijskoj godini u slučaju kada se radi o poduzeću:

a) Osnovni principi obrade, uključujući uvjete za pristanak, u skladu s Člancima 5, 6 7 i 9;

Članak 5. objašnjava principe obrade osobnih podataka:

1. Osobni podaci će biti:

f) Obrađeni na način koji osigurava odgovarajuću sigurnost osobnih podataka, uključujući zaštitu od neovlaštene ili nezakonite obrade te slučajnog gubitka, uništenja ili oštećenja, uz primjenu odgovarajućih tehničkih ili organizacijskih mjera ('integritet i povjerljivost').

Neke od zemalja članica su već počele raditi na usklađivanju s GDPR regulativom. Na primjer, Nizozemska je u svibnju 2015. godine izmijenila Zakon o zaštiti podataka, čime je njen režim zaštite podataka postao jednim od najstrožih u Europi. GDPR regulativa stupa na snagu u svim zemljama članicama Europske unije u svibnju 2018. godine.

KOJE MJERE JE POTREBNO PODUZETI ODMAH?

Regulativa zahtijeva od institucija da uvedu nove procese i pravila radi pružanja veće kontrole nad osobnim podacima privatnih osoba. Ovo uključuje pisanje novih pravila i uputa, obučavanje osoblja i obnavljanje sistema radi izvršavanja novih procedura. Drugi koraci uključuju praktične mjere kao što je uvođenje enkripcije podataka.

Izgubljeno ili ukradeno prijenosno računalo ili USB stick ne moraju dovesti do kazne ukoliko su podaci na njima bili šifrirani odobrenim proizvodom. Jedan od proizvođača koji nude odobrene programe za zaštitu podataka je i ESET sa svojim DESlock alatima za enkripciju koji posjeduju FIPS 140-2 validaciju.

Jedan od ključnih principa GDPR regulative je osiguravanje odgovarajuće razine sigurnosti osobnih podataka. Kao što je navedeno u Članku 32, enkripcija predstavlja odgovarajuću tehničku mjeru za ostvaranje ovog cilja. U slučajevima kada se enkripcija koristi kao tehnička mjera, neophodno je osigurati mogućnost povrata podataka u slučaju incidenta. Također je neophodno voditi pismenu evidenciju o poduzetim mjerama u svojstvu dokaza da su sistemi sigurni te da je moguć povrat podataka.

DESlock rješenja tvrtke ESET su dizajnirana kako bi efikasno ispunila ove zahtjeve. U nastavku se nalazi pregled nekih funkcija DESlock-ovih proizvoda koji osiguravaju ispunjavanje standarda za zaštitu osobnih podataka u skladu s GDPR regulativom:

Cilj	ESET-ova DESlock enkripcija
Osiguravanje podataka u mirovanju	Sve komercijalne verzije DESlock enkripcije uključuju mogućnost enkripcije datoteka, mapa i izmjenjivih medija radi zaštite podataka na korisničkim uređajima.
Osiguravanje podataka u prijenosu	DESlock+ Pro uključuje mogućnost pune enkripcije diska i izmjenjivih medija radi osiguravanja podataka u prijenosu
Osiguravanje podataka tijekom rada od kuće	Komercijalne DESlock licence dozvoljavaju drugu instalaciju na privatnim uređajima. Pored toga, DESlock+ Go omogućuje uređivanje kriptiranih dokumenata na USB uređajima.

Cilj	ESET-ova DESlock enkripcija
Siguran prijenos podataka između lokacija	Sve verzije DESlock programa uključuju plug-in za Outlook i enkripciju clipboard-a kompatibilnu sa svim klijentima e-pošte, uključujući webmail, te enkripciju priloga pošte za sve sustave. Enkripcija optičkih medija omogućuje siguran prijenos podataka na CD ili DVD diskovima.
Blokiranje/ograničavanje pristupa određenim podacima	Jedinstvena i patentirana tehnologija dijeljenja ključeva omogućuje jednostavno upravljanje pravima pristupa podacima u složenim timovima i radnim grupama.
Dopuštanje pristupa sigurnim podacima na zahtjev.	DESlock+ Enterprise Server je dizajniran za udaljeno upravljanje putem sigurne internetske veze. Ključevi se mogu brzo dijeliti i opozivati s centralne lokacije.
Sigurno spremanje osobnih podataka	DESlock enkripcija ispunjava FIPS-140-2 standard te koristi pouzdane, provjerene i sigurne algoritme i metode enkripcije.
Uništavanje nepotrebnih podataka	DESlock+ alat za uništavanje digitalnih dokumenata nepovratno uništava podatke u skladu s DoD-5220.22-M standardom, čime osigurava da se jednom uništeni podaci ne mogu vratiti.

Više informacija

Opće informacije:

https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2015/15-12-08_Truste_speech_EN.pdf

Pojedinosti regulative

http://www.statewatch.org/news/2015/dec/eu-council-dp-reg-draft-final-compromise-15039-15.pdf

Tekst direktive o zaštiti privatnih podataka u slučaju pravosudnih postupaka

http://www.statewatch.org/news/2015/dec/eu-council-dp-dir-leas-draft- final-compromise-15174-15.pdf