ZAKONI ZA ZAŠTITU PODATAKA U 2018. I NADALJE

Razmatranja tehnologije u pozadini sve veće sigurnosti informacija

Canon

Sadržaj

“

Ne možemo pobjeći od činjenice da je od 2018. godine nastupilo izazovno razdoblje u zaštiti podataka i upravljanju rizicima povezanima s informacijama uslijed promjenljivog regulatornog okruženja koje nastavlja izravno utjecati na poslovni uspjeh. Prema mom mišljenju, napredovat će organizacije koje prihvate poslovni model utemeljen na podacima i poduzmu nužne promjene kako bi sigurnost informacija stavile u središte svega što rade, bilo da se radi o IT rukovoditeljima ili upravitelju odbora.

Quentyn Taylor, direktor za sigurnost informacija, Canon Europe Ltd

Sigurnost informacija u digitalnom svijetu može biti zastrašujući pothvat. Velika brzina tehnoloških inovacija potaknula je stvaranje jednako promjenljivog regulatornog okruženja dok sukladnost drži korak s pojavom interneta stvari (IoT), masovnih podataka, digitalne transformacije i mnogobrojnih drugih trendova koji mijenjaju lice poslovanja i ureda diljem Europe. Budući da se informacije kreću brže nego ikad prije i na više uređaja, sigurno rukovanje njima bez narušavanja svakodnevnih zadataka od ključne je važnosti za tvrtke svih veličina u svim djelatnostima.

Dok su pojedinosti o slučajevima neovlaštenih pristupa podacima velikih razmjera dominirale vijestima posljednjih mjeseci i godina, pretjerana buka oko Opće uredbe o zaštiti podataka (OUZP, engl. GDPR) podigla je razinu strategija i IT infrastrukture u pozadini zaštite podataka klijenata. Iako je to općenito dobra stvar, važno je napomenuti da su iznimno sofisticirani kibernetički napadi rijetki, a "jednostavniji" (ali ništa manje štetni) neovlašteni pristupi podacima, kao što su izgubljeni mobilni telefoni, dokumenti ostavljeni u odlagačima pisača ili zaobilaženje uredske opreme u korist potrošačke tehnologije jednako opasni za integritet podataka organizacije.

Štoviše, tvrtke moraju shvatiti da se potreba za sigurnošću ne odnosi isključivo na jedan odjel ili djelatnost. Tu na scenu stupaju posebni propisi, a time i analize utemeljene na podacima, radi određivanja rizičnih korporacijskih kultura. Bilo da se radi o certificiranim sigurnosnim standardima ili velikim zakonskim promjenama, tvrtke imaju odgovornost razumjeti što se od njih očekuje u pravnom smislu ili u suprotnom snositi teške posljedice po rad, ugled i financije.

Ovaj vodič kroz zakonske propise usredotočuje se na najveće promjene u propisima o zaštiti podataka u 2018., način na koji se propisi mogu odnositi na vašu tvrtku i, ako se odnose, način na koji možete poduzeti prve korake ka sukladnosti.

Osmišljen je da tvrtkama pomogne razumjeti potrebe za sukladnosti koje utječu na njihov svijet, kao i da im pomogne u donošenju boljih i informiranijih odluka za poslovanje. Osim toga, trebao bi i omogućiti timovima da prepoznaju koliko su voljni riskirati, gdje su granice tolerancije za rizik i kako najbolje upravljati tim varijablama.

Od prosinca 2017., više od polovine europskih poduzeća (52 %) nije znalo kakav će učinak GDPR imati na njihovo poslovanje.[1]

OPĆA UREDBA O ZAŠTITI PODATAKA (GDPR)

Što je to?
U svibnju 2018. godine, Opća uredba EU-a o zaštiti podataka (GDPR) zamijenila je Direktivu o zaštiti podataka iz 1995. godine. Novi zakon, osmišljen kako bi pojedincima omogućio veću kontrolu nad njihovim osobnim podacima, ujednačio je zaštitu podataka u cijeloj Europskoj uniji i zahtijeva da sve tvrtke koje djeluju unutar nje imaju određene mjere za zaštitu podataka. To uključuje nova pravila kako bi se osigurala otpornost sustava i usluga za obradu privatnih informacija, sposobnost poduzeća da obnavljaju i pristupaju podacima u slučaju kršenja, kao i česta testiranja i procjene učinkovitosti.

Promjene također donose stroži sustav kazni, što znači da bi u slučaju prekršaja organizacije mogle biti kažnjene novčanom kaznom do 4 % svoga ukupnog godišnjeg prometa ili 20 milijuna eura – što god je veće.

Međutim, ne smije se previdjeti prilika koju GDPR donosi. U svijetu koji prolazi kroz digitalnu transformaciju, za mnoge je tvrtke već odavno potrebna revizija podataka, a za mnoge je krajnji rok koji ih je plašio zapravo bio potrebni katalizator za kulturne i operativne promjene. To im je omogućilo da zamijene naslijeđene sustave i osuvremene načine rada modernim, digitalnim, čak i automatiziranim procesima koji donose operativnu učinkovitost i vlastite suvremene radne prakse.

1. www.eset.com/int/business/gdpr-low-level-implementation-according-idc-report

25. svibnja 2018. .
Iako je već postala zakonom, 25. svibnja 2018. nova je uredba službeno stupila na snagu i od tog trenutka tvrtke se mogu suočiti s kaznama za nepoštivanje.

Na koga to utječe?
GDPR se primjenjuje na sva poduzeća – velika i mala, u svakoj djelatnosti – koja imaju pristup povjerljivim podacima koji pripadaju građaninu EU-a. To obuhvaća bivše, postojeće pa čak i potencijalne kupce, klijente, dobavljače i zaposlenike.

Prema IDC-u, 40 % ljudi ne razumije što je GDPR, a 62 % nije sigurno odnosi li se na tiskane dokumente.[2]

Kako ispuniti zahtjeve odredbi
Datum obvezne usklađenosti bio je 28. svibanja 2018., tako da tvrtke sada trebaju doista razumjeti kako se nova pravila GDPR-a odnose na njih, kao i korake koje moraju poduzeti.

- **Izradite program za ostvarivanje usklađenosti** – Postavite skup pravila, procedura i kontrola za praćenje usklađenosti. To bi trebalo uključivati doprinos iz svih područja poslovanja, od odjela za ljudske resurse i IT-a do viših rukovoditelja, i trebao bi djelovati kao prva postaja prilikom procjene ili kvantificiranja rizika.

- **Budite transparentni u obradi podataka** – tvrtke trebaju ažurirati obavijesti o privatnosti i dijeliti te informacije sa svim pojedincima čije osobne podatke (PII) imaju. To mora biti u skladu s pravnim parametrima GDPR-a i ne zaboravite uzeti u obzir 5 pitanja – zašto se podaci prikupljaju? Tko ih prikuplja? Gdje će biti pohranjeni? Kakav to učinak ima na pojedinca? I kada će isteći?

- **Uspostavite protokole za izvješćivanje** – Tvrtke imaju 72 sata za prijavu kršenja podataka u slučajevima u kojima pojedinac može biti pogođen. Ključno je da informatički odjeli budu svjesni procesa u slučaju povrede podataka. Povrede podataka su neizbježne, ali se šteta može povećati ako tvrtke ne postupaju na pozitivan način. To započinje proaktivnim izvješćivanjem i učinkovitom komunikacijom s regulatorima i pogođenim stranama.

- **Obrazujte svoju radnu snagu** – GDPR utječe na cijelu organizaciju. Svi pojedinci moraju razumjeti kojim osobnim podacima svakodnevno rukuju, kako se to usklađuje s novim propisima i posljedice koje se mogu pojaviti ako se ti podaci tretiraju na način koji nije u skladu s poslovnim pravilima o sigurnosti podataka. Zapamtite, svaka tvrtka ima drugačiju sklonost riskiranju, stoga nije dovoljno pretpostaviti da je od svibnja 2018. svatko upoznat s GDPR-om i razumije ga.

2. IDC Western Europe Hardcopy Survey, 2. kvartal 2017.

To znači da više od 50 % tvrtki do kraja 2018. godine nije uspjelo u potpunosti ispuniti zahtjeve GDPR-a, ocijenio je Gartner.[3]

Što su osobni podaci?

GDPR se primjenjuje na "osobne podatke", što znači bilo koju informaciju koja se odnosi na osobu koja se može izravno ili neizravno identificirati. To uključuje osobne podatke koji se čuvaju na digitalnim i ručnim sustavima arhiviranja.

U praksi će širok raspon identifikatora predstavljati osobne podatke, uključujući ime, identifikacijski broj zaposlenika, lokaciju, pa čak i e-adresu.

Osobni podaci koji uključuju pseudonime – npr. informacije koje su promijenjene u numeričke podatke – mogu spadati u opseg GDPR-a ovisno o tome koliko je teško pripisati pseudonim određenom pojedincu.

3. www.gartner.com/newsroom/id/3701117

KAKO GDPR UTJEČE NA IT TIMOVE?

Podatkovna strategija
Kako bi se osigurala usklađenost, IT profesionalci trebaju biti svjesni svakog odjela unutar svoje organizacije koji rukuje privatnim podacima, kao i toga gdje ih pohranjuju. To uključuje provjeru platformi za svrhe kao što su marketing, pa čak i usluge u oblaku. Uspostava odgovarajuće IT infrastrukture nužna je kada je u pitanju praćenje uporabe podataka te će također pomoći u definiranju sigurnosne strategije tvrtke, zajedno s drugim preventivnim metodama, uključujući enkripciju, provjeru autentičnosti s više čimbenika, zaštitu zaporkom i stroga pravila uporabe vlastitog uređaja (BYOD).

Pristup podacima
Čim se poduzeće susreće s osobnim podacima, postaje odgovorno za način uporabe tih podataka. Dok bi krajnji korisnici trebali biti redovito informirani o važnosti usklađenosti, bilo bi nepromišljeno misliti da se pogreška ne može dogoditi. IT odjeli bi stoga trebali razmotriti kako prate uporabu podataka, primjerice uvođenjem kontrole zaposlenika koji imaju pristup podacima, kako bi im pomogli da zadovolje nove sigurnosne standarde. To bi valjalo primjenjivati i kada se radi s trećim stranama, uključujući obrađivače podataka koji će se vjerojatno koristiti redovito.

Nadzor podataka
Možemo reći da je GDPR dobrano zaposlio IT timove, a s novim procedurama obavješćivanja o kršenju, potreba za istinskom sigurnošću podataka ne pokazuje znakove usporavanja. Razmislite o proširenju tima i angažiranju stručnjaka za sigurnost. To ne bi pomoglo samo kod svakog stalnog nadzora, već bi i ponudilo veću stručnost prilikom upozoravanja poduzeća na potencijalni rizik ili kršenje podataka. Bilo da imate tu mogućnost ili ne, nužno je ulagati u nove ili ažurirane IT programe, posebno one koji mogu pružiti uvid o tome kako se podaci upotrebljavaju.

Procjenjuje se da će globalna ulaganja u financijske tehnologije premašiti 150 milijardi dolara u narednih tri do pet godina[4]

DRUGA DIREKTIVA O PLATNIM USLUGAMA (PSD2)

Što je PSD2?
Revolucija u industriji plaćanja u svjetlu velikih tehnoloških pomaka tijekom proteklog desetljeća, Druga direktiva o platnim uslugama (PSD2) predstavlja ažuriranje početne Direktive EU-a o platnim uslugama. Uključujući nekoliko novih zahtjeva, druga iteracija osmišljena je kako bi se suočila s monopolom tradicionalnih banaka nad podacima o potrošačima u uslugama za građanstvo, u doba kada inovacije i konkurencija u financijskoj tehnologiji (fintech) brzo rastu.

Otvoreno bankarstvo omogućuje pružateljima usluga iniciranja plaćanja (PISP) – primjerice tvrtkama kao što je Amazon – i pružateljima usluga pružanja informacija o računu (AISP), kao što je europska aplikacija za osobne financije Tink, dobivanje podataka o klijentovom računu iz njegove banke pod uvjetom da imaju njegov pristanak. To u suštini znači da se korisnici ne preusmjeravaju na servise kao što je PayPal prilikom plaćanja stvari na mreži.

Kada je riječ o sigurnosti, PSD2 ovlašćuje prethodno neregulirane PISP-ove i AISP-ove da postanu pružatelji platnih usluga (PSP). Ti novi PSP-ovi moraju osigurati primjenu odgovarajućih sigurnosnih mjera i procesa, kao što je provjera autentičnosti s više čimbenika, a istovremeno raditi prema međunarodnim sigurnosnim propisima i standardima, uključujući GDPR i standard za sigurnost podataka (PCI-DSS).

Od tvrtki se može zahtijevati da značajno osuvremene svoje postojeće okvire, podijeljene u tri glavna problemska područja: upravljanje operativnim i sigurnosnim rizicima, provjera autentičnosti i izvješćivanje. Ako to ne učine, odgovarajuća država članica može izreći kazne.

Zakonodavstvo bi moralo pomoći da banke učinkovitije služe korisnicima te korisnicima omogućiti bolji uvid u njihov financijski život.

4. https://press.pwc.com/News-releases/traditional-financial-services-firms-fear-almost-a-quarter-of-their-business-is-at-risk-from-fintech/s/F3F3DEA5-CBF9-4B0D-AFF2-164F418E6451

Ključni datum
PSD2 je stupio na snagu 13. prosinca 2016., što je državama članicama dalo dvogodišnji rok za prijenos u nacionalno zakonodavstvo.

Od 13. siječnja 2018. godine, poduzetnici na koje se odnosi ovaj zakon moraju djelovati u skladu s novim tehničkim standardima.

Banke i pružatelji usluga platnog prometa također bi morali biti svjesni da neke sigurnosne mjere, uključujući pravila o jakoj provjeri autentičnosti i sigurnoj komunikaciji, Europska komisija nije usvojila istovremeno pa stoga imaju vlastite vremenske okvire. U tom slučaju, rujan 2018. bio je najraniji datum usvajanja u kojem su mogli stupiti na snagu.

Na koga utječe PSD2?
S obzirom da je djelatnost platnih usluga već podložna zahtjevima direktive PSD2, tvrtke – posebno banke – susrećeu se sa smanjenjem prihoda ako ne počnu diversificirati svoje poslovne modele i prihvaćati nove mogućnosti koje PSD2 može ponuditi.

Banke | **Tvrtke za financijske tehnologije** | **Davatelji platnih usluga** | **Davatelji telekomunikacijskih usluga** | **Maloprodaja**

Banke
Bankarski je sektor u središtu digitalne revolucije, jer startupi inovativnih financijskih tehnologija ruše tradicionalni model i decentraliziraju bankarske usluge za građanstvo, pa čak i investicijsko bankarstvo.

Prema direktivi PSD2, banke su tim pružateljima trećih strana dužne pružati pristup računima svojih klijenata putem otvorenih API-ja (sučelja za programiranje aplikacija). To omogućuje trećim stranama da izgrade financijske usluge na temelju bankovnih podataka i infrastrukture.

Financijske tehnologije
PSD2 je pomogao da se izjednači područje industrije, kao i da se otvori obilje mogućnosti za financijske tehnologije (fintechs). U tolikoj mjeri da, osim izgradnje partnerstva s većim ustanovama kao što su banke, otvoreno bankarstvo također potiče pojavljivanje novih tehnologija. Primjerice, PIS-ovi rade uzbudljiv posao u područjima kao što su instant plaćanja.

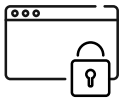
Sigurnost bi morala biti glavni prioritet za tvrtke s financijskim tehnologijama koje žele napredovati, pogotovo stoga što agencija Financial Conduct Authority odobrava samo one s potrebnim tehničkim standardima.

Poslovni korisnici
Poslovni korisnici imat će jednake koristi od direktive PSD2, odnosno moći će koristiti integriranije usluge, gdje su podaci o računu ugrađeni u različite platforme. Najveća briga za tvrtke trebala bi biti osiguravanje sigurnosti svojih podataka putem pouzdanih odnosa, budući da prema novom zakonu više tvrtki ima pristup informacijama, što povećava broj potencijalnih mjesta kršenja.

Kad se radi o važnim financijskim informacijama, kadrovske resurse često mogu potrošiti vremenski zahtjevni administrativni poslovi. Tvrtke bi trebale razmotriti racionalizaciju tih procesa automatiziranjem određenih financijskih funkcija i upravljanjem zadacima na središnjoj razini. To bi također trebalo dovesti do poboljšane poslovne učinkovitosti tijekom vremena.

Obavezna uporaba otvorenih API-ja uzrokuje značajne izazove za financijske institucije. Infrastruktura mora odgovoriti na ove nove propise otvorenom, pristupačnom, prilagodljivom i fleksibilnom IT arhitekturom. Međutim, mnoge su organizacije otkrile da ovaj otvoreni pristup IT-u stvara širok raspon poslovnih prilika.

Preporučuje se dugoročno ulaganje u tehnologiju, posebno s obzirom na to da će na tržištu plaćanja i dalje biti povećane razine konkurencije. To znači odabir IT sustava koji će nuditi prednosti kroz više godina, a ne kratkoročno rješenje. Razgovarajte s rukovodstvom poduzeća i dogovorite zajamčeni proračun pa isprobajte više sustava kako biste pronašli one koji najviše odgovaraju vašoj spremnosti na rizik i istovremeno jamče rad kakav vaše poduzeće treba.



Kakav je utjecaj na IT?
PSD2 nedvojbeno donosi određenu količinu tehnološkog rada za institucije na koje se odnosi. Agilnije organizacije i one iz digitalne generacije mogu imati prednost pred API-jima, ali će možda trebati i poboljšati svoje aktivnosti u svjetlu direktive PSD2. Etablirane banke vjerojatno su stigle dalje uz API-je nego što bi se moglo misliti, ali budući da moraju ostvariti dodatni razvoj u kraćem vremenu, možda će trebati istražiti strategije koje će im pomoći da nadoknade zaostatak na najučinkovitiji način. Također im ne gine povezivanje starih sustava i podataka s tim novim uslugama.

Ključni izazov u smislu tehničkih mogućnosti proizlazi iz provjere autentičnosti, budući da institucije moraju identificirati klijente u svim platformama i organizacijama.

Novi propisi snažno su utjecali na voditelje informatičkih odjela (CIO) diljem Europe. Oni koji se mogu i žele brzo kretati mogli bi iskoristiti te promjene kao priliku za ubrzavanje otvorenog bankarstva i digitalizacije. Revidirana Direktiva o platnim uslugama prisiljava banke i organizacije da podjednako nude otvoreni pristup podacima i transakcijama etabliranim tržišnim igračima i novim akterima: otvaranje uz dužnu sigurnost pada na teret IT odjela.

PSD2 i otvoreno bankarstvo
Otvoreno bankarstvo je trend koji se brzo razvija u financijskim uslugama i industriji financijskih tehnologija. Radi se o poslovnom pristupu temeljenom na platformi, gdje su podaci, procesi i poslovne funkcionalnosti dostupni ekosustavu kupaca, razvojnih inženjera, fintech početnika ili partnera. PSD2 uklanja prepreke budući da dijeljenje računa i informacija o plaćanju postaje obavezno.

Djelatnosti s najboljim rezultatima po pitanju sukladnosti s PCI standardom[5]:

- **IT usluge** (61,3 %)
- **Financijske usluge**(59,1 %)
- **Ugostiteljstvo** (50 %)
- **Maloprodaja** (42,9 %)

PCI STANDARD ZA SIGURNOST PODATAKA (PCI-DSS)

Što je to?
Vijeće za sigurnosne standarde industrije kartičnog plaćanja (Payment Card Industry Security Standards Council) nastoji održati sigurnost plaćanja unutar svake organizacije koja pohranjuje, obrađuje ili prenosi podatke vlasnika kartice. Osmišljen kao skup tehničkih i operativnih zahtjeva za one koji prihvaćaju ili obrađuju plaćanja, u velikoj se mjeri usredotočuje i na tehnologiju i softver koji se upotrebljava u transakcijama.

U svijetu u kojem kriminalci i prevaranti upotrebljavaju sve sofisticiranije tehnologije za dobivanje podataka o vlasnicima kartica, važno je da trgovci i financijske ustanove redovito nadziru bilo kakve sigurnosne propuste – ne samo zato što mogu imati dalekosežne posljedice po vlasnike kartica. Neovlašteni pristupi u ovom slučaju mogu i narušiti kredibilitet tvrtki čija je jedina svrha sigurna obrada informacija o plaćanju.

Tvrtke koje ne zadovolje ove standarde mogle bi dobiti velike kazne te se suočiti sa sljedećim:

- Pad poslovanja i prodaje
- Troškovi zamjene platnih kartica
- Potencijalni pravni troškovi
- Globe i kazne za nesukladnost
- Uskraćivanje mogućnosti primanja platnih kartica

Ključni datum
1. veljače 2018. godine tvrtke su dobile zadatak da promijene svoje upravljačke procese kako bi potvrdile da su zahtjevi standarda PCI-DSS zadovoljeni nakon znatnih promjena.

30. lipnja 2018. godine predstavljao je rok za onemogućavanje protokola SSL (Secure Socket Layer) i implementiranje sigurnijeg protokola za šifriranje kako bi se zadovoljili zahtjevi standarda PCI-DSS za zaštitu podataka o plaćanju.

Na koga će to utjecati?
Sve tvrtke koje pohranjuju, obrađuju ili prenose podatke vlasnika kartice.

Što bi tvrtke trebale poduzimati za osiguravanje sukladnosti?
Vijeće za sigurnosne standarde industrije kartičnog plaćanja (PCI Security Standards Council) utvrdilo je tri jednostavna koraka[6] na putu tvrtki prema sukladnosti koja bi se trebala tretirati kao stalni ciklus.

Procjena – Identifikacija podataka o vlasnicima kartica, popisivanje IT sredstava i poslovnih procesa za obradu platnih kartica te njihovo analiziranje radi utvrđivanja ranjivosti

Popravljanje – Popravljanje ranjivosti i uklanjanje pohrane podataka o vlasnicima kartica ako nije nužno potrebna

Izvješćivanje – Sastavljanje i slanje potrebnih izvješća odgovarajućoj banci i kartičnim kućama

Koji je utjecaj na IT?
IT odjeli koji upotrebljavaju sigurne sustave plaćanja i rješenja bit će u najboljem položaju po pitanju ostvarivanja sukladnosti zahtjevima standarda PCI. U nastavku se navode preporuke uz koje tvrtke mogu održati najviše razine sigurnosnih standarda:

- **Održavanje sigurne mreže**
  Ovo treba obuhvaćati sva područja mrežne sigurnosti, od brige o tome da je na sustav instaliran najnoviji antivirusni softver do promjene zaporki dobivenih od dobavljača

- **Kreiranje sustava za upravljanje rizikom**
  Surađujte s različitim odjelima tvrtke kako biste kreirali i uveli sigurnosna pravila na temelju rizika na koje ste voljni pristati, uključujući proces utvrđivanja neovlaštenog pristupa i izvješćivanja o njemu

- **Zaštita podataka vlasnika kartica**
  Primijenite višeslojnu provjeru autentičnosti za one koji žele pristupiti podacima o vlasniku kartice, kao što su ograničeni pristup na temelju njihovog položaja u tvrtki i jedinstveni ID-ovi za prijavu za svakog korisnika

- **Dosljedno i temeljito testiranje**
  Osigurajte redovit nadzor protokola za zaštitu podataka tijekom cijele godine kao dio stalnog sigurnosnog procesa

5. http://www.verizonenterprise.com/resources/2017_payment_security_report_technical_report_en_xg.pd
5. https://www.pcisecuritystandards.org/pci_security/how

ISO SIGURNOSNI STANDARD 27002

ISO 27002 međunarodni je standard najboljih praksi za sigurnost informacija, kako ga definira Međunarodna organizacija za standardizaciju (International Organisation for Standardisation – ISO). Djelujući kao skup praksi za koje se izdaje certifikat, temelji se na obaveznim zahtjevima prvi put definiranima standardom ISO 27001, a bavi se s tri aspekta provođenja informacijske sigurnosti tvrtki: ljudi, proces i tehnologija.

Za tvrtke koje žele implementirati, poboljšati ili održavati svoje sigurnosne procedure, sukladnost ISO sigurnosnom standardu nije obavezna, ali može osigurati prednosti najbolje prakse. Osim toga, uvjerava klijente i korisnike da se rizicima adekvatno upravlja.

Budući da se ne radi o pravnom zahtjevu, treba razmotriti vrijeme i troškove povezane s angažiranjem zaposlenika, opreme za nadzor i (često velikih) revizijskih naknada. No, i to ulaganje treba uzeti u obzir u odnosu na prihod od novih klijenata koji cijene ISO certifikaciju, kao i povećanja prodaje.

Na koga će to utjecati?
Utjecati će na svaku tvrtku koja želi raditi unutar najboljih standarda za sigurnost informacija. Za urede diljem EMEA područja, ISO predstavlja zlatni standard sigurnosti.

Kao tvrtka, kako ga možemo iskoristiti?

- **Bolje upravljanje rizikom** i mogućnost prepoznavanja prijetnji sigurnosti
- Dobro dizajniran i temeljit program za zaštitu informacija **smanjuje troškove** cijele tvrtke
- **Stvaranje pouzdanja kod korisnika** po pitanju sigurnosti njihovih podataka
- Usvajanje najboljih međunarodnih standarda sigurnosti može pomoći tvrtkama **da zadovolje zakonske zahtjeve**
- **Dobivanje pristupa novim korisnicima** u različitim djelatnostima

98 % organizacija kaže da su obavezni zahtjevi standarda ISO 27001 poboljšali informacijsku sigurnost[7]

7. www.itgovernance.co.uk/download/ISO27001-Global-Report-2016.pdf

Što je najbitnije za IT odjel?
Kao što vrijedi za sve propise o zaštiti podataka, dobro razvijena IT infrastruktura od ključne je važnosti ako tvrtke žele postići sigurnosne standarde potrebne za ISO certifikaciju. To znači da su IT odjeli, uz više rukovoditelje, u središtu razvoja sustava upravljanja informacijskom sigurnošću (Information Security Management System – ISMS).

Odredite opseg: Tvrtka najprije mora odrediti podatke koje će ISMS obuhvaćati i tehnologiju koju ima spremnu kao podršku. Bitno je razmotriti i potrebe i zahtjeve trećih strana (klijenata, vlasnika udjela, zaposlenika itd.).

Implementirajte nužne kontrole: Utvrdite kontrole potrebne za maksimalno smanjenje rizika po tvrtku na najbolji način i usporedite ih s najboljim praksama koje predlaže ISO.

Unaprijedite razinu upućenosti zaposlenika: Identificirajte istaknute zaposlenike i one koji su odgovorni za njih. Uputite te korisnike u potencijalne prijetnje, ranjivosti i utjecaj gubitka povjerljivosti, integriteta i dostupnosti. Moderan ured prepun je povezanih uređaja i usluga, a sve bi one trebale doprinositi kulturi učinkovitosti i inteligentnog, mobilnog rada. Međutim, veći broj uređaja i veća količina podataka u uredu donose izazove za informacijsku sigurnost. Od ključne je važnosti obučiti zaposlenike o rizicima i njihovom doprinosu dobrim praksama po pitanju podataka.

Nastavite nadzor: Pobrinite se da ISMS nastavlja slijediti međunarodni standard tako da redovito pratite i pregledavate njegovu učinkovitost. Time bi se trebao ostvariti proces stalnog poboljšanja. Razine prijetnji stalno se razvijaju, uredska se tehnologija mijenja, a hakeri postaju sve snalažljiviji. Mirovanje jednostavno ne dolazi u obzir.

ZAKLJUČAK

Osiguravanje sukladnosti s propisima o zaštiti podataka nije mali zadatak, naročito zato što zahtijeva djelovanje na gotovo svim razinama tvrtke. Budući da se podaci svakodnevno kontroliraju, pohranjuju, obrađuju i dijele na više različitih platformi, sustava i procesa, tvrtke ponekad zaboravljaju da IT odjel nije dovoljan za osiguravanje njihove zaštite.

Međutim, kao što smo vidjeli, te promjene donose prilike. Vidjeli smo tek početak projekata digitalne transformacije diljem svijeta. Uz zakonske promjene koje se tiču strukture, zaštite i dostupnosti podataka iz 2018. godine i ubuduće, tvrtke imaju priliku ponovno osmisliti neke od svojih najvažnijih protokola za integritet tih informacija

Zakonodavne su promjene neizbježne jer se tehnologija razvija i iziskuje različite razine upravljanja.

No, čak i bez zakonskih okvira, zaštita podataka postala je važnija nego ikad prije. Kako tvrtke svih oblika i veličina sve više iskorištavaju podatke, rizik povezan s pogrešnim rukovanjem podacima, bilo da je štetan po financije ili ugled, nikad nije bio jasniji. Općenito, korisnici rado dijele svoje podatke s tvrtkama u zamjenu za bolja, povezana iskustva, ali to povjerenje brzo može nestati ako tvrtke nisu u mogućnosti zaštititi osobne podatke.

Mnogo se promjena odvija u svim djelatnostima, ali nude se i ogromne prilike. Na zakone se ne bi trebalo gledati kao na ograničavanje napretka ili inovacija, nego kao na važan preduvjet za njihovo dugoročno omogućavanje.

Želite saznati više?

Ako želite dodatne informacije, posjetite www.canon.hr/business/gdpr-psd2-compliance-guide

O tvrtki Canon Europe

Canon pruža najveći portfelj uredskih uređaja na tržištu i može podržavati sve tehnologije uređaja – pojedinačne i višefunkcijske, male i širokog formata – s pomoću svog softvera za upravljanje mrežom. Bliska veza između naših hardverskih i softverskih tehnologija poboljšava našu mogućnost zaštite dokumenata kako se kreću i prolaze kroz svoj informacijski ciklus trajanja.

Canon Europe podružnica je tvrtke Canon Inc. za EMEA regiju, globalnog davatelja tehnologija i usluga za obradu slike te jedne od najprepoznatljivijih i najpopularnijih robnih marki na svijetu. Canon Europe djeluje u približno 120 država, zapošljava približno 19 000 ljudi diljem regije i donosi oko trećinu Canonovog godišnjeg prihoda na globalnoj razini.

Dodatne informacije o tvrtki Canon Europe dostupne su na:
www.canon-europe.com

Canon Inc.
canon.com

Canon Europe
canon-europe.com

Croatian edition 0147W156

Canon Croatia d.o.o.
Kovinska 4a
10090 Zagreb
Hrvatska
Tel:+ 385 1 5579 843
Fax: + 385 1 5579 856
canon.hr

/Canon
/Canon
/CanonBusinessUK