RUKOTVORINA

RUKOTVORINA j.d.o.o. za proizvodnju i trgovinu
Vinički put 20 - 47000 Karlovac
GSM: 095/ 2516670
tel.fax.: 047/ 600967
mail: rukotvorina@ka.t-com.hr
OIB: 06872137311 - MB: 04076656

U Karlovcu, 23.05.2018.

AKCIJSKI PLAN OSTVARIVANJE SUKLADNOSTI S ODREDBAMA GDPR

1. IZRADA PROJEKTA

Pripremi za GDPR se mora pristupiti kao projektu, s toga je potrebno tim zaposlenika uključi u pripremni dio. Financije, knjigovodstvo, prodaja, marketing i IT služba. To su dijelovi koji će doći u kontakt sa obradom osobnih podataka.
Jednom kada se skupi tim potrebno je postaviti točne ciljeve i rokove u kojima pojedini dijelovi tvrtke moraju izvršiti prilagodbu.

2. PODIGNUTI RAZINU SVJESNOSTI O GDPR-u

Trebati će potpora SVIh zaposlenika s obzirom da će promjene uvelike utjecati na rad cijele tvrtke. Ne može se samo slati jedan mail, potrebna je cijela kampanja. Da li je potrebno da voditelj poslovanja nauči sve detalje koje mora znati osoba koja vrši prodaju ? Što želite da ljudi pročitaju iz vaših poruka? FAQ je dobar način da pripremite svoj cijeli tim.

3. ANALIZIRAJTE SVOJE PODATKE

Razumljivo je da ne možete zaštiti ono što ne poznajete. Ovisno o veličini vaše tvrtke potrebno je različito vrijeme da se analiza izvrši. Najbolje je da sa anketom započnete skupljanje informacija.
Pošaljite anketu svih voditeljima poslovanja i obavezno neka anketa sadrži slijedeća pitanja:

- Tko je odgovoran za zaštitu podataka u vašem odjelu?
- Koji osobni podaci se obrađuju u vašem odjelu?
- Da li čuvate „osjetljive“ osobne podatke, ukoliko da molim nabrojite?
- Koja je svrha obrade osobnih podataka?
- Kako ste došli do osobnih podataka ? Marketingom, preko trećih osoba ili sl.?
- Gdje i kako čuvate osobne podatke ? Na službenom serveru, na Cloud-u, na prijenosnim računalima, u papirnatom obliku ili drugačije ?
- Otprilike koliko osobnih podataka imate ?
- Da li ste predvidjeli rok čuvanja osobnih podataka, ako da navedite koliko ?
- Da li dijelite te podatke sa trećim osobama ili izvan RH ?
- Da li je vaš odjel prošao tečaj primjene GDPR-a ?

Ono što pokušavate dobiti putem analize je uvid u moguće rizike kod obrade osobnih podataka. Što veći broj anketa uspijete sakupiti dobiti ćete bolji uvid u obradu osobnih podataka u vašoj tvrtki.

4. ŠTO DALJE ?

Sada kada ste dobili uvid u količinu osobnih podataka, morate razumjeti količinu dokumenata koje trebate izraditi da biste iste zaštitili. Ovaj dio također pripada analizama pošto pokušavamo pronaći „rupe“ u procedurama i poduzeti radnje da iste zakrpamo da ne dolazi do curenja informacija.
Sastavite popis politika, procedura i ugovora koje imaju bilo kakvu vezu na obradu OP (osobnih podataka):

- Ugovori sa zaposlenicima
- Ugovori sa dobavljačima
- Politika zaštite tajnosti poslovanja
- Popis podataka u računalu
- Privole
- dosadašnje procedure zaštite osobnih podataka

5. RECI ŠTO VIDIŠ

Zasigurno već imate Pravilnik o obradi osobnih podataka kojega ste dosada koristili da biste objasnili zašto skupljate osobne podatke od ispitanika i za što čete iste koristiti. Sada isti pravilnik morate proširiti da ispitanik zna da li ćete njegove podatke podijeliti s trećim osobama i na koji način mogu se dodatno informirati o količini podataka koje imate o pojedinom ispitaniku.
Takvi podaci se često nalaze u ugovorim o poslovnoj suradnji ili ugovorima o radu s zaposlenicima, s toga pregledajte ugovore i po potrebi ih aneksima proširite za tražene podatke.

6. „JA IMAM PRAVA“ reče ispitanik

Prava ispitanika moraju postati temelj prilikom obrade osobnih podataka. Prava ispitanika su:

- Pravo na informiranost – čl.12 do čl.14
- Pravo na pristup – čl.15
- Pravo na ispravak – čl.16
- Pravo na brisanje podataka – „pravo da budem zaboravljen“ čl.17
- Pravo na odbijanje davanja privole – čl.18
- Pravo na prijenos podataka – čl.20
- Pravo na prigovor – čl.21
- Pravo da se obrada ne vrši automatizmom – čl.22

Prema GDPR-u svatko tko skuplja OP mora imati zakonsku osnovu na temelju koje vrši obradu osobnih podataka, morate svakako provjeriti da li je to tako u vašoj tvrtki, a ako nemate pravnu osnovu morate imati vrlo dobar razlog da to činite.
Ali pazite … ako vršite obradu podataka na temelju privole onda ispitanik ima pravo da zahtjeva brisanje ili može koristiti pravo na prijenos podataka.

Pa, zbog čega vi skupljate OP ?

7. NEKA BUDE LEGALNO

Prvo načelo GDPR-a je da se obrada vrši zakonito, pošteno i transparentno s obzirom na ispitanika. To znači da morate imati legalni razlog za prikupljanje OP i postoje šest razloga kada smijete vršiti obradu nečijih OP. Detaljno ih obrađuje čl.6 i glase:

- ispitanik je dao privolu za obradu svojih osobnih podataka u jednu ili više posebnih svrha
- obrada je nužna za izvršavanje ugovora u kojem je ispitanik stranka ili kako bi se poduzele radnje na zahtjev ispitanika prije sklapanja ugovora

- obrada je nužna radi poštovanja pravnih obveza voditelja obrade – propisana je drugim zakonom
- obrada je nužna kako bi se zaštitili ključni interesi ispitanika ili druge fizičke osobe
- obrada je nužna za izvršavanje zadaće od javnog interesa ili pri izvršavanju službene ovlasti voditelja obrade;
- obrada je nužna za potrebe legitimnih interesa voditelja obrade ili treće strane, osim kada su od tih interesa jači interesi ili temeljna prava i slobode ispitanika koji zahtijevaju zaštitu osobnih podataka, osobito ako je ispitanik dijete

Privola je najosjetljiviji od gore navedenih točaka, jer u trenutku nadzora potrebno je dokumentirati i dokazati da je privola stvarno i dobivena. To se prvenstveno odnosi na marketinške odjele unutar tvrtke.

8. ŠTO NAPRAVITI AKO SE NEŠTO LOŠE DOGODI ?

Morate si razjasniti što morate napraviti u slučaju da „procure“ podaci, jer čete biti u grdoj nevolji ako ne izvršite prijavu unutar 72 sata od trenutka incidenta.
Svakako da ćete sve učiniti što vam je u vašoj moći da zaštitite OP – educirati ćete svoje zaposlenike, vršiti redovni back-up podataka i osigurati tehničku zaštitu – no onda vam netko zabije nož u leđa i pošalje email sa osjetljivim podacima na pogrešno mjesto – i na vama je da to sada objasnite. A ako nemate spreman proces upravljanja incidentima da brzom reakcijom objasnite nastalu situaciju AZOP-u ili ispitaniku čiji su podaci „procurili“, naći čete se na udaru ogromnim kaznama a da ne govorimo o gubitku poslovne reputacije.

Pitanje koje si postavljamo sada je : Da li imamo proces upravljanja incidentima ? Ako da, svakako ga treba revidirati da budemo sigurni da li pokriva ne samo fizičke incidente (krađu ili gubitak podataka), nego i tehničke incidente (hakerski napad npr.).

Svakako je u ovom trenutku bitno da imate osobu – Službenika za zaštitu osobnih podataka – koji će izvršiti uvid u incident i mora znati kako da procjeni d ali je potrebno o incidentu izvijestiti AZOP ili ispitanika, s obzirom da postoje situacije kada to nije potrebno (npr. kada su podaci kriptirani ili pseudomizirani). Da liste planirali imati takvu osobu i tko će to biti ?

9. SLUŽBENIK ZA ZAŠTITU OSOBNIH PODATAKA

GDPR je izuzetno detaljno opisao vještine i znanje koje službenik mora imati, koja je njegova pozicija u GDPR-u i koji su njegovi zadaci. Također postoje situacije kada ga uopće ne treba imenovati, što je sve pokriveno čl.37 – 39 Uredbom.

Prvi korak je da odlučite da li trebate ili morate imati Službenika za GDPR ?
Morate ga imati u slijedećim situacijama:

- obradu provodi tijelo javne vlasti ili javno tijelo, osim za sudove koji djeluju u okviru svoje sudske nadležnosti
- osnovne djelatnosti voditelja obrade ili izvršitelja obrade sastoje se od postupaka obrade koji zbog svoje prirode, opsega i/ili svrha iziskuju redovito i sustavno praćenje ispitanika u velikoj mjeri, ili
- osnovne djelatnosti voditelja obrade ili izvršitelja obrade sastoje se od opsežne obrade posebnih kategorija podataka na temelju članka 9. i osobnih podataka u vezi s kaznenim osudama i kažnjivim djelima iz članka 10.

Ukoliko službenika ne morate imati morate dokumentirati svoje razloge. No u svakom slučaju, ako se i odlučite da nećete imenovati službenika za GDPR, trebate nekoga koji će biti zadužen da izvrši sve potrebne analize obrade jer će se sigurno desiti da netko želi ostvariti svoja prava iz GDPR i trebati će vam netko da obradi zahtjev ispitanika.

10. PRAVO NA PRISTUP INFORMACIJAMA

U prijašnjim zakonima o zaštiti podataka također je postojala mogućnost da osoba zatraži i dobije uvid u obim osobnih podataka koje vaša tvrtka ima o njemu. Bilo koji zahtjev morate shvatiti ozbiljno bilo da ste ga zaprimili mailom, poštom, osobno ili telefonski. Rok za odgovaranje na upite ispitanika je 1 mjesec s toga ….

OVIH DESET KORAKA ĆE VAS DOVESTI BLIŽE CILJU DA BUDETE USKLAĐENI S GDPR-om, NO NAJČEŠĆE KADA SE KREĆE U IZRADU DOKUMENTACIJE, CIJELI NIZ PITANJA SE JOŠ DODATNO OTVARA, S OBZIROM DA JE POTREBNO DA SE ZA SVE TVRTKE DOKUMENTACIJA PRILAGODI S OBZIROM NA KOLIČINU OSOBNIH PODATAKA, DJELATNOSTI TVRTKE I OBIMU OBRADE.