

AUDIT PRIPRAVENOSTI PO REALIZÁCIÍ OPATRENÍ PRE SÚLAD S GDPR

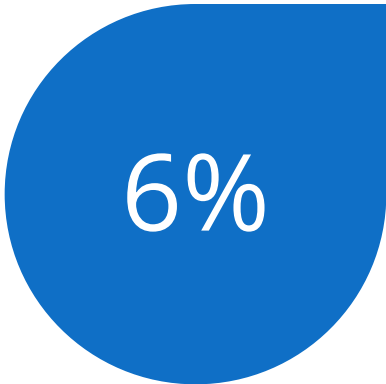
Klaudia Göndörövä

Ako sa zmení optika po 25 máji 2018?

- ROZŠÍRENIE POJMU OSOBNÝ ÚDAJ (ZARADENIE MEDZI OSOBNÉ ÚDAJE NAPR. IP ADRESU, COOKIES)
- NOVÉ POJMY AKO PROFILOVANIE, PSEUDONYMIZÁCIA, ANONYMIZÁCIA
- PORUŠENIE OCHRANY OSOBNÝCH ÚDAJOV A POVINNOSŤ OHLÁSIŤ INCIDENT DO 72 HODÍN DOZORNÉMU ORGÁNU
- NOVÉ POJMY HLAVNÁ PREVÁDZKAREŇ, ZÁSTUPCA, SKUPINA PODNIKOV
- NOVÉ PODMIENKY UPLATNITEĽNÉ NA SÚHLAS DIEŤAŤA V SÚVISLOSTI SO SLUŽBAMI INFORMAČNEJ SPOLOČNOSTI
- NOVÉ PODMIENKY PRE POVINNOSŤ VYMENOVAŤ ZODPOVEDNÚ OSOBU
- NOVÉ PODMIENKY PRE POVINNOSŤ VYPRACOVAŤ POSÚDENIE VPLYVU NA OCHRANU ÚDAJOV
- NOVÁ DOKUMENTÁCIA K SPRACOVATEĽSKÝM ČINNOSTIAM
- ROZŠÍRENIE PRÁV DOTKNUTÝCH OSÔB
- DOPLNENÝ OBSAH SPROSTREDKOVATEĽSKEJ ZMLUVY NA OCHRANU OSOBNÝCH ÚDAJOV,
- ZRIADENIE EURÓPSKEHO VÝBORU PRE OCHRANU OSOBNÝCH ÚDAJOV
- NOVÉ ZDRUŽENIA A INÉ SUBJEKTY ZASTUPUJÚCE KATEGÓRIE PREVÁDZKOVATEĽOV ALEBO SPROSTREDKOVATEĽOV MÔŽU VYPRACOVAŤ KÓDEXY SPRÁVANIA
- MONITOROVANIE SCHVÁLENÝCH KÓDEXOV SPRÁVANIA
- ZAVEDENIE CERTIFIKAČNÝCH MECHANIZMOV OCHRANY ÚDAJOV A PEČATÍ A ZNAČIEK OCHRANY ÚDAJOV NA ÚČELY PREUKÁZANIA SÚLADU S NARIADENÍM

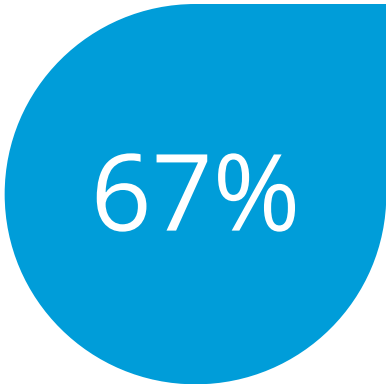


AKO JE NA TOM TRH?



6%

Len 6% firiem je plne pripravených na účinnosť všeobecného nariadenia Európskej únie o ochrane údajov (GDPR)



67%

67% globálnych firiem sa domnieva, že zrejme nespĺnila termín na uplatnenie GDPR



2/3

Dve tretiny organizácií nie sú pripravené na „právo na zabudnutie“

AKO ĎALEKO V IMPLEMENTÁCIÍ STE VY?

ETAPA STRATÉGIA GDPR:

1. BUDOVANIE POVEDOMIA
2. STRATÉGIA GDPR
3. GAP ANALÝZA

ETAPA IMPLEMENTÁCIA GDPR:

4. KLASIFIKÁCIA
5. FUNKČNÉ POŽIADAVKY
6. PRACOVNÉ POSTUPY

ETAPA KONTINUÁLNEHO ZLEPŠOVANIA GDPR:

7. RIADENIE RIZÍK
8. OPATRENIA
9. AUDIT
10. CERTIFIKÁCIA

AKO NA TO?

DOSTUPNOSŤ DOKUMENTÁCIE

- GAP analýza
- Návrh opatrení

ETAPA IMPLEMENTÁCIA GDPR: SÚČINNOSŤ DOTKNUTÝCH ÚTVAROV

- Zodpovedná osoba
- Business vlastníci
- Bezpečnostný manažér

METODIKA CMMI (CAPABILITY MATURITY MODEL INTEGRATION) - STANOVENIE SPÔSOBILOSTI PROCESOV A VYSPELOSTI ORGANIZÁCIE

AKO NA TO?

Stupeň		Hodnota a popis	Popis úrovne	Hodnotené atribúty				
				Funkcia	Činnosť	Dokumentácia	Roly/Zodpovednosť	Monitorovanie/Meranie/Kontrola
0	0,0		Činnosť nie je vykonávaná . Neexistuje dokumentácia. Nie sú definované role a zodpovednosti. Nie je vykonávané meranie ani kontrola.	Nezabezpečená alebo zabezpečená minimálne	Nevykonávaná alebo vykonávaná minimálne	Neexistuje alebo je nedostatočná, neúplná, nejasná	Nedefinované, neúplné	Nevykonávané
1		Vykonávanie						
	0,1	Minimálne	Opatrenia/mechanizmy sú vykonávané a realizované AD HOC ; Neexistuje dokumentácia. Nie sú definované role a zodpovednosti. Nie je vykonávané meranie ani kontrola.					
	0,2	Čiastočne	Opatrenia/mechanizmy sú vykonávané a realizované AD HOC ; Dokumentácia nie je vypracovaná, ale je naúplná a nedostatočná; Nie sú definované role a zodpovednosti. Nie je vykonávané meranie ani kontrola.	Zabezpečená AD HOC	Vykonávané AD HOC, náhodne	Existuje len základná, všeobecná, bez popisu mechanizmov	Prideľované AD HOC	Náhodné, neriadené
	0,3	Úplne	Opatrenia/mechanizmy sú vykonávané a realizované AD HOC ; Dokumentácia nie je vypracovaná, alebo je naúplná a nedostatočná; Zodpovednosť je prideľovaná AD HOC; Meranie a kontrola je iba náhodná;					
2		Popis						
	0,4	Minimálne	Opatrenia/mechanizmy sú popísané minimálne a realizujú sa; Dokumentácia je len formálna, ale nie je dostatočná, pravidlá sú ústne alebo nedostatočne popísané; Zodpovednosť a roly sú definované ústne, neformálne, ale nie sú riadené; Monitorovanie a kontrola nie sú popísané a sú vykonávané nepriamo;					
	0,5	Čiastočne	Opatrenia/mechanizmy sú popísané čiastočne a realizujú sa; Dokumentácia je len formálna, štrukturálne úplná, podporuje politiku, pravidlá sú ústne alebo nedostatočne popísané, obsahovo nedostatočná; Zodpovednosť a roly sú definované ústne, neformálne a vykonávané v súlade s politikou a sú riadené; Monitorovanie a kontrola nie sú popísané a sú vykonávané nepriamo;	Plánovaná a zabezpečená v súlade s politikou, monitorovaná, riadená. Pravidlá nie formalizované	Plánovaná a vykonávaná v súlade s politikou, riadená, Pravidlá nie sú formalizované	Je len formálna, štrukturálne úplná, podporuje politiku, pravidlá sú ústne alebo nedostatočne popísané, obsahovo nedostatočná	Definované len čiastočne alebo ústne, vykonávané v súlade s politikou, riadené	Nepopísané, nemeria sa priamo
	0,6	Úplne	Opatrenia/mechanizmy sú popísané úplne a realizujú sa; Dokumentácia je len formálna, štrukturálne úplná, podporuje politiku, pravidlá sú ústne alebo nedostatočne popísané, obsahovo nedostatočná; Zodpovednosť a roly sú definované a vykonávané v súlade s politikou a sú riadené; Monitorovanie a kontrola nie sú popísané a sú vykonávané nepriamo;					

AKO NA TO?

Stupeň		Hodnota a popis	Popis úrovne	Hodnotené atribúty				
				Funkcia	Činnosť	Dokumentácia	Roly/Zodpovednosť	Monitorovanie/Meranie/Kontrola
0	0,0		Činnosť nie je vykonávaná . Neexistuje dokumentácia. Nie sú definované role a zodpovednosti. Nie je vykonávané meranie ani kontrola.	Nezabezpečená alebo zabezpečená minimálne	Nevykonávaná alebo vykonávaná minimálne	Neexistuje alebo je nedostatočná, neúplná, nejasná	Nedefinované, neúplné	Nevykonávané
1		Vykonávanie						
	0,1	Minimálne	Opatrenia/mechanizmy sú vykonávané a realizované AD HOC ; Neexistuje dokumentácia. Nie sú definované role a zodpovednosti. Nie je vykonávané meranie ani kontrola.					
	0,2	Čiastočne	Opatrenia/mechanizmy sú vykonávané a realizované AD HOC ; Dokumentácia nie je vypracovaná, ale je naúplná a nedostatočná; Nie sú definované role a zodpovednosti. Nie je vykonávané meranie ani kontrola.	Zabezpečená AD HOC	Vykonávané AD HOC, náhodne	Existuje len základná, všeobecná, bez popisu mechanizmov	Prideľované AD HOC	Náhodné, neriadené
	0,3	Úplne	Opatrenia/mechanizmy sú vykonávané a realizované AD HOC ; Dokumentácia nie je vypracovaná, alebo je naúplná a nedostatočná; Zodpovednosť je prideľovaná AD HOC; Meranie a kontrola je iba náhodná;					
2		Popis						
	0,4	Minimálne	Opatrenia/mechanizmy sú popísané minimálne a realizujú sa; Dokumentácia je len formálna, ale nie je dostatočná, pravidlá sú ústne alebo nedostatočne popísané; Zodpovednosť a roly sú definované ústne, neformálne, ale nie sú riadené; Monitorovanie a kontrola nie sú popísané a sú vykonávané nepriamo;					
	0,5	Čiastočne	Opatrenia/mechanizmy sú popísané čiastočne a realizujú sa; Dokumentácia je len formálna, štrukturálne úplná, podporuje politiku, pravidlá sú ústne alebo nedostatočne popísané, obsahovo nedostatočná; Zodpovednosť a roly sú definované ústne, neformálne a vykonávané v súlade s politikou a sú riadené; Monitorovanie a kontrola nie sú popísané a sú vykonávané nepriamo;	Plánovaná a zabezpečená v súlade s politikou, monitorovaná, riadená. Pravidlá nie formalizované	Plánovaná a vykonávaná v súlade s politikou, riadená, Pravidlá nie sú formalizované	Je len formálna, štrukturálne úplná, podporuje politiku, pravidlá sú ústne alebo nedostatočne popísané, obsahovo nedostatočná	Definované len čiastočne alebo ústne, vykonávané v súlade s politikou, riadené	Nepopísané, nemeria sa priamo
	0,6	Úplne	Opatrenia/mechanizmy sú popísané úplne a realizujú sa; Dokumentácia je len formálna, štrukturálne úplná, podporuje politiku, pravidlá sú ústne alebo nedostatočne popísané, obsahovo nedostatočná; Zodpovednosť a roly sú definované a vykonávané v súlade s politikou a sú riadené; Monitorovanie a kontrola nie sú popísané a sú vykonávané nepriamo;					

AKO NA TO?

3	Kontrola							
	0,7	Minimálne	Opatrenia/mechanizmy sú popísané úplne a realizujú sa; Dokumentácia je úplná, riadená a sú jasne popísané činnosti; Zodpovednosti a role sú definované, pokryté ľudskými zdrojmi, popísané, podporené internou legislatívou; Monitorovanie a kontrola sú popísané, čiastočne pokryté ľudskými zdrojmi, popísané, podporené internou legislatívou, vykonávané AD HOC;					
	0,8	Čiastočne	Opatrenia/mechanizmy sú popísané úplne a realizujú sa; Dokumentácia je úplná, v súlade so štandardami, riadená a sú jasne popísané činnosti; Zodpovednosti a role sú definované, pokryté ľudskými zdrojmi, popísané, podporené internou legislatívou; Monitorovanie a kontrola sú popísané, pokryté ľudskými zdrojmi, popísané, podporené internou legislatívou, čiastočne vykonávané; Prebieha proces čiastočného zlepšovania;	Plánovaná a zabezpečená v súlade s politikou, monitorovaná, riadená, kontrolovaná Pravidlá sú formalizované internými predpismi	Zadefinovaná v politike, plánovaná a vykonávaná podporená internými predpismi	Je obsahovo úplná, riadená, striktné podporuje politiku, jasne popísané činnosti	Definované, pokryté, popísané, podporené internými predpismi	Definované, vykonávané, pokryté, popísané, podporené internými predpismi
	0,9	Úplne	Opatrenia/mechanizmy sú popísané úplne a realizujú sa; Dokumentácia je úplná, v súlade so štandardami, riadená a sú jasne popísané činnosti; Zodpovednosti a role sú definované, pokryté ľudskými zdrojmi, popísané, podporené internou legislatívou; Monitorovanie a kontrola sú popísané, pokryté ľudskými zdrojmi, popísané, podporené internou legislatívou, vykonávané; Prebieha proces zlepšovania;	kvantitatívne ciele, sa pravidelne vyhodnocujú	kvantitatívne ciele, sa pravidelne vyhodnocujú	revízie dokumentácie sú pravidelne vykonávané a vyhodnocované	definované zodpovednosti osôb sú merateľné a aj sa merajú a vyhodnocujú	vyhodnocované voči merateľným ukazovateľom
	1	Neustále zlepšovanie	Opatrenia/mechanizmy sú plne popísané a realizujú sa; Dokumentácia je úplná a v súlade so štandardami, riadená a sú jasne popísané činnosti; Zodpovednosti a role sú definované, pokryté ľudskými zdrojmi, popísané, podporené internou legislatívou; Monitorovanie a kontrola sú popísané, pokryté ľudskými zdrojmi, popísané, podporené internou legislatívou, plne vykonávané; Prebieha proces kontinuálneho zlepšovania;					

GDPR A EMM, A PREČO NIE?

Vieme Vám pomôcť s rôznymi oblasťami:

- **Audit súladu**
- **Technologické opatrenia**
 - DLP
 - Klasifikácia dokumentov
 - Šifrovanie
 - GDPR App



Máme referencie od klientov v oblasti bankovníctva, poisťovníctva, ...



DISKUSIA

Otázky môžete klásť aj cez **sli.do**
Zadajte slido.com do Vášho prehliadača
Zadajte kód eventu **#EMMBB**