Implementácia *MegaLAN*

U nás je to jednoduché

je to super ale musí to tiež byť:

- transparentné (pre dozorný úrad a fyzickú osobu, ktorej dáta sa spracovávajú)
- dokladovateľné (pre dozorný úrad)
- v súlade s GDPR, ale tiež ďalšími zákonmi (zákonník práce, zákony o zdravotnom, sociálnom, dôchodkovom zabezpečení a ďalšími poisteniami, kybernetickej bezpečnosti, antispamovým atd.)
- musia byť pokrytí všetci dodávatelia – mzdová účtáreň, právne poradenstvo, personálne agentúry, externe spolupracujúci špecialisti, ktorí majú prístup k osobným údajom...

Čo implementácia predstavuje?

- uvedenie interného a externého spracovánia os. údajov do súladu s nariadeniami GDPR
- nastavenie organizačných opatrení, aktualizácia vnútornej predpisovej bázy
- procesné úpravy riadiace spracovávanie a povinnosti
- nastavenie spracovávania požiadaviek osôb, ktorých os. údaje sa spracovávajú
- popis a realizacia úprav informačných systémov
- zmluvné a organizačné pokrytie ext. spracovateľov, dodávateľov a pod.
- spracovanie registrov os. údajov, registra účelov spracovania atď.
- uskutočnenie balančných testov a povinných posúdení vplyvov na dopad práv osôb
- zabezpečenie dokladovateľnosti súladu voči dozornému úradu
- vypracovanie kódexu správania

Ako implementácia prebieha

- quick scan - úvodná analýza určujúca rozsah projektu
- GAP analýza – zistenie, čo všetko sa musí implementovať
- dopadová analýza – určenie toho, čo to bude znamenať pre firmu (napr. úpravy metodík, vytvorenie metodík, prezmluvnenie dodavateľov, zmena zmlúv so zamestnancami,…)
- návrh business riešenia
- detailná analýza dát
- detailná analýza procesov
- IT implementacia
- finální audit

Ako dlho implementácia prebieha

- podľa veľkosti a typu organicácie
- podľa typu podnikania – napr. pri firmách B2B je to kratšia doba ako pri B2C
- od 1 mesiaca vo firme s niekoľkými zákazníkmi, až do niekoľkých rokov vo firmách s tisíckami zamestnancov
- rozsah tiež úzko súvisí s požadovanou úrovňou implementácie tj. aké riziká majú byť pokryté a aké nie

Projektové (dokumentové) výstupy

- návrh riešení – dokument popisujúci konkrétnu implementáciu v organizácii vychádzajúci z následujúcich dokumentov a analýz
  - *GAP analýza – analýza rozdielu medzi aktuálnym stavom organizácie a stavom cieľovým*
  - *Impact analýza – analýza dopadov na organizáciu*
  - *dátová analýza – popis spracovávaných os. údajov a ich kategorizácia*
  - *procesná analýza – popis procesov alebo ich častí zameraných (výlučne) na spracovanie os. údajov*
  - *analýza IT systémov – analýza IT aplikácií, ich integrácia a nutné úpravy, ktorých výstupom je zadanie k implementácii*
  - *register aplikacií, register dodavateľov (v rozsahu nevyhnutnom pre implementaciu GDPR a podľa konkrétnej situácie v organizácii)*
- finálny audit

MegaLAN

PARTNER PRE IMPLEMENTÁCIU GDPR

General Data Protection Regulation
(Regulation (EU) 2016/679)

Nariadenie Európskeho parlamentu a Rady Európskej únie, ktorého cieľom je harmonizácia pravidiel ochrany osobných údajov v krajinách Európskej únie. Prísnejšie pravidlá týkajúce sa ochrany fyzických osôb pri spracúvaní osobných údajov a voľnom pohybe týchto údajov znamená, že občania budú mať väčšiu kontrolu nad svojimi údajmi a podniky budú využívať výhody z rovnakých trhových podmienok. Jeden súbor pravidiel pre všetky spoločnosti pôsobiace v EU bezohľadu na to kde majú sídlo.

Čo je to GDPR? Prečo ho implementovať?

- zákonná povinnosť stanovená nariadením Európského parlamentu a Rady (EU) 2016/679
- jedná sa o právny predpis priamo aplikovateľný vo všetkých krajinách EU
- účinnost je od 25. mája 2018
- na Slovensku dôjde k nahradeniu doteraz platného zákona o ochrane osobných údajov č. 122/2013 Z.z.

Pôsobnosť nariadenia

- v prípade komerčných subjektov akékoľvek spracovanie osobných údajov /OÚ/
- spracovávaním sa rozumie aj zhromaždovanie, evidencia a archivácia OÚ
- miestna pôsobnosť v krajinách EU; miestach, kde sa uplatňuje právo na základe medzinárodného a v prípade ponúk alebo služieb subjektom v EU

Prehľad noviniek */čo je nové v ochrane osobných údajov/*

- rozšírenie definície OÚ
- požiadavky na zabezpečenie – design by default
- výrazné posilnenie práva osôb voči správcovi – prevádzkovateľovi OÚ
- zvýšená informačná povinnosť spracovateľov
- oznamovacia povinnosť aj v prípade narušenia zabezpečenia
- vyššia ochrana detí
- kódexy správania a osvedčenie súladu spracovánia os. údajov podľa GDPR
- zodpovedná osoba pre ochranu OÚ ako nová nezávislá funkcia vo firme

Pojem osobný údaj

- všetky informácie o identifikovanej fyzickej osobe
- zvláštne kategórie /predtým citlivé/ – vyžadujú vyšší stupeň ochrany
- množstvo technických identifikátorov (sieťové identifikátory, IP adresy, cookies…)
- zvláštna kategória OÚ, najmä biometrické a genetické údaje, údaje o zdravotnom stave

/okrem zvláštnej kategórie OÚ je kategória osobných údajov zakázaných spracovávať - údaje o rase, náboženstve, politickom presvedčení , sexuálnej orientácii, členstve v odboroch a pod./

Požiadavky na spracovanie

- zákonnosť, korektnosť a transparentnosť
- účelové obmedzenie – iba na základe legálneho účelu
- minimalizácia údajov – údaje bez účelu nie je možné uchovávať
- presnosť
- limit na uloženie
- integrita a dôveryhodnosť
- zodpovednosť organizácie za spacovanie v súlade s GDPR
- povinnosť organizácie aktívne preukazovať súlad s GDPR

MegaLAN

10. HLAVNÝCH DOPADOV GDPR

01 | Zabezpečenie osobných údajov a narušenie bezpečnosti

- by design – musí byť už v návrhu , by default – štandardne musí byť zapnuté
- organizácia musí zaviesť vhodné opatrenia na ochranu os. údajov napr. anonymizácia alebo pseudoanonymizácia údajov z dôvodu minimalizácie posúvaných údajov
- organizacia má povinnosť hlásiť porušenie zabezpečenia dozornému úradu
- súčasťou musí byť popis incidentov, jeho dôsledky, rozsah a prijaté opatrenia
- lehota je maximálne do 72 hodin!!!

02 | Menovanie zodpovednej osoby za ochranu O.Ú.

- DPO – data protection officer
- v organizáciách s väčším počtom zamestnancov
- priamo podriadená vrcholovému vedeniu
- nesmie dostávať úlohy priamo od vedenia spoločnosti
- musí poskytovať interné poradenstvo
- musí monitorovať sulad s GDPR
- musí spolupracovať s dozorovým orgánom
- môže byť interná aj externá

03 | Súhlas so spracovaním

- jeden zo spôsobov legalizácie spracovania osobných údajov
- získanie súhlasu musí byť organizáciou doložiteľné
- súhlas musí byť slobodný a informovaný
- zreteľne oddelený od zmluvy či iného dokumentu
- osoba môže súhlas kedykoľvek jednostranne odvolať

/Každý z vyššie uvedených bodov je v GDPR špecifikovaný ako má byť realizovaný alebo za akých podmienok/

04 | Cezhraničné spracovanie mimo EU

- sú vyžadované vhodné záruky napr. záväzné podnikové pravidlá, kódexy a osvedčenia
- v niektorých prípadoch povolenie dozorných úradov

05 | Práva osôb

- právo na prístup k údajom
- právo na informácie
- právo na vysvetlenie
- právo na odstránenie závadného stavu
- právo na obmedzenie spracovania
- právo na ľudský zásah v prípade rozhodnutia na báze automatizovaného spracovania
- právo na výmaz
- právo na prenositelnosť osobných údajov k inej organizácii (aj konkurenčnej)
- právo vzniesť námietku

06 | Profilovanie a automatizované spracovanie

- osoba má právo nebyť predmetom žiadneho spracovania založeného výhradne na automatizovanom spracovaní, vrátane profilovania, ktoré má na osobu potenciálne právne následky
- profilovaním sa rozumie vyhodnocovanie správania osoby

07 | Externé spracovanie

- spracovateľ musí poskytovať dostatočné záruky, že dáta budu spracovávané v súlade s GDPR
- súčasťou je zaistenie ochrany údajov osôb
- je nutné mať - spracované pokyny pre externého spracovateľa
  - mlčanlivosť
  - súčinnosť pri spracování požiadaviek osôb
  - priame oznamovanie bezpečnostných incidentov
- reťazenie spracovateľov je možné len s výslovným súhlasom organizácie, pre ktorú sú osobé údaje spracovávané

08 | Anonymizácia a pseudoanonymizácia

- množstvo spravovávaných osobných údajov musí byť minimalizované
- je potrebné zaviesť opatrenia, ktoré zabránia prístupu k údajom, ktoré nie sú nutné pre spracovanie
- týmito opatreniami sú anonymizácia a pseudoanonymizácia
- anonymizácia predstavuje takú úpravu O.Ú., ktorá nezvratne znemožní identifikovať osobu
- pseudonymizácia osobných údajov je proces skrytia identity, ktorého účelom je mať možnosť zbierať dalšie údaje týkajúce sa osoby, aby nebolo nutné poznať jeho totožnosť – typicky šifrovaním za pomoci kľúča

09 | Kodex správania a certifikácia

- je zavedený kódex správania organizácie
- týka sa aj spracovateľov
- je to verejný dokument
- kódex musí preukazovať plnenie povinností organizácie vyplývajúcich z GDPR
- je dobrovoľný, ale súčasne je to jeden z mála nástrojov ako preukázať súlad s GDPR

10 | Posúdenie vplyvu na ochranu osobných údajov

- je to metodický postup v prípade spracovávania O.Ú. s vysokým rizikom na práva osôb
- súčasťou musí byť popis a vyhodnotenie rizík
- v prípade potvrdenia rizík musia byť popísané opatrenia, ktoré tieto riziká zmierňujú
- musí to byť konzultované s dozorným úradom, ktorý má právo spracovanie zakázať
- v prípade zmeny je nutné prieskum opakovať!

BONUS: Sankcie pri nesplnení

- maximálny strop je 10 milionov EUR, alebo 2% celkového ročného svetového obratu
- pri závažných porušeniach strop 20 milionov EUR, alebo 4% celkového ročného obratu
- uplatní sa vždy vyššia čiastka