



PARTNER PRE IMPLEMENTÁCIU GDPR

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



Čo je to GDPR? Prečo ho implementovať?

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.

- **ZÁKONNÁ POVINNOSŤ STANOVENÁ NARIADENÍM EURÓPSKEHO PARLAMENTU A RADY (EU) 2016/679**
- **JEDNÁ SA O PRÁVNY PREDPIS PRIAMO APLIKOVATEĽNÝ VO VŠETKÝCH KRAJINÁCH EÚ. ÚČINNOSŤ JE OD 25. MÁJA 2018**
- **NA SLOVENSKU DÔJDE K NAHRADENIU DOTERAZ PLATNÉHO ZÁKONA O OCHRANE OSOBNÝCH ÚDAJOV Č. 122/2013 Z.Z V ZNENÍ NESKORŠÍCH PREDPISOV.**





PÔSOBNOSŤ NARIADENIA

- V PRÍPADE KOMERČNÝCH SUBJEKTOV AKÉKOL'VEK SPRACOVÁVANIE OS. ÚDAJOV
- SPRACOVÁVANÍM SA ROZUMIE AJ ZHROMAŽĎOVANIE, EVIDENCIA A ARCHIVÁCIA OSOBNÝCH ÚDAJOV
- MIESTNA PÔSOBNOSŤ V KRAJINÁCH EÚ, MIESTACH KDE SA UPLATŇUJE PRÁVO NA ZÁKLADE MEDZINÁRODNÉHO A V PRÍPADE PONÚK, ALEBO SLUŽIEB SUBJEKTOM V EÚ





PREHL'AD NOVINIEK

- ROZŠÍRENIE DEFINÍCIE OSOBNÝCH ÚDAJOV
- POŽIADAVKY NA ZABEZPEČENIE – BY DESIGN, BY DEFAULT
- VÝRAZNÉ POSILNENIE PRÁVA OSÔB VOČI SPRÁVCOVI – PREVÁDZKOVATEĽOVI OS. ÚDAJOV
- ZVÝŠENÁ INFORMAČNÁ POVINNOSŤ SPRACOVATEĽOV
- OZNAMOVACIA POVINNOSŤ AJ V PRÍPADE NARUŠENIA ZABEZPEČENIA
- VYŠŠIA OCHRANA DETÍ
- KÓDEXY SPRÁVANIA A OSVEDČENIE SÚLADU SPRACOVÁVANIA OS. ÚDAJOV PODĽA GDPR
- ZODPOVEDNÁ OSOBA PRE OCHRANU OSOBNÝCH ÚDAJOV 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 OSOBNÝCH ÚDAJOV , NAJMA BIOMETRICKÉ A GENETICKÉ ÚDAJE, ÚDAJE O ZDRAVOTNOM STAVE

Okrem zvláštnej kategórie os. údajov je kategória os. 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 SPRACOVANIE V SÚLADE S GDPR
- POVINNOSŤ ORGANIZÁCIE AKTÍVNE PREUKAZOVAŤ SÚLAD S GDPR



10. HLAVNÝCH DOPADOV GDPR

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



1. 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
- ORGANIZÁCIA MÁ POVINNOSŤ HLÁSIŤ PORUŠENIE ZABEZPEČENIA DOZORNÉMU ÚRADU
- SÚČASŤOU MUSÍ BYŤ POPIS INCIDENTOV, JEHO DÔSLEDKY, ROZSAH A PRIJATÉ OPATRENIA
- LEHOTA JE MAXIMÁLNE DO 72 HODIN!!!



2. MENOVANIE ZODPOVEDNEJ OSOBY ZA OCHRANU OSOBNÝCH ÚDAJOV

- 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 SÚLAD S GDPR
- MUSÍ SPOLUPRACOVAŤ S DOZOROVÝM ORGÁNOM
- MOŽE BYŤ INTERNÁ AJ EXTERNÁ



3. SÚHLAS SO SPRACOVANÍM

- JEDEN ZO SPÔSOBOV LEGALIZÁCIE SPRACOVANIA OS. ÚDAJOV
- ZÍSKANIE SÚHLASU MUSÍ BYŤ ORGANIZÁCIOU DOLOŽITEĽNÉ
- SÚHLAS MUSÍ BYŤ SLOBODNÝ A INFORMOVANÝ
- ZRETEL'NE 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



4. CEZHRANIČNÉ SPRACOVANIE MIMO EÚ

- SÚ VYŽADOVANÉ VHODNÉ ZÁRUKY NAPR. ZÁVÄZNÉ PODNIKOVÉ PRAVIDLÁ, KÓDEXY A OSVEDČENIA
- V NIEKTORÝCH PRÍPADOCH POVOLENIE DOZOROVÝCH ÚRADOV



5. 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 PRENOS OS. ÚDAJOV K INEJ ORGANIZÁCII (AJ KONKURENČNEJ)**
- **PRÁVO VZNIEŠŤ NÁMIETKU**



6. 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



7. 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 SPRACOVANÍ POŽIADAVIEK OSÔB
 - PRIAME OZNAMOVANIE BEZPEČNOSTNÝCH INCIDENTOV
- REŤAZENIE SPRACOVATEĽOV JE MOŽNÉ LEN S VÝSLOVNÝM SÚHLASOM ORGANIZÁCIE PRE KTORÚ SÚ OS. ÚDAJE SPRACOVÁVANÉ



8. ANONYMIZÁCIA A PSEUDOANONYMIZÁCIA

- MNOŽSTVO SPRACOVÁVANÝCH OS. ÚDAJOV MUSÍ BYŤ MINIMALIZOVANÉ
- JE POTREBNÉ ZAVIESŤ OPATRENIA, KTORÉ ZABRÁNIA PRÍSTUPU K ÚDAJOM, KTORÉ NIE SÚ NUTNÉ PRE SPRACOVANIE
- TAKÝMITO OPATRENAMI SÚ ANONYMIZÁCIA A PSEUDOANONYMIZÁCIA
- ANONYMIZÁCIA PREDSTAVUJE TAKÚ ÚPRAVU OS. ÚDAJA, KTORÁ NEZVRATNE ZNEMOŽNÍ IDENTIFIKOVAŤ OSOBU
- PSEUDOANONYMIZÁCIA OSOBNÝCH ÚDAJOV JE PROCES SKRYTIA IDENTITY, KTORÉHO ÚČELOM JE MAŤ MOŽNOSŤ ZBIERAŤ ĎALŠIE ÚDAJE TÝKAJÚCE SA OSOBY, ABY NEBOLO NUTNÉ POZNAŤ JEHO TOTOŽNOSŤ – TYPICKY ŠIFROVANÍM ZA POMOCI KLÚČA



9. KÓDEX 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 DOBROVOLNÝ, 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 OS. ÚDAJOV 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 DOZOROVÝM ÚRADOM, KTORÝ MÁ PRÁVO SPRACOVANIE ZAKÁZAŤ
- V PRÍPADE ZMENY JE NUTNÉ POSÚDENIE OPAKOVAŤ!



BONUS: SANKCIE PRI NESPLNENÍ

- MAXIMÁLNY STROP JE 10 MILIÓNOV EUR, ALEBO 2% CELKOVÉHO ROČNÉHO SVETOVÉHO OBRATU
- PRI ZÁVAŽNÝCH PORUŠENIACH STROP 20 MILIÓNOV EUR, ALEBO 4% CELKOVÉHO ROČNÉHO OBRATU
- UPLATNÍ SA VŽDY VYŠŠIA ČIASTKA



IMPLEMENTÁCIA MEGALAN

S NAMI JE TO JEDNODUCHÉ



JE TO SUPER, ALE MUSÍ TO TIEŽ BYŤ:

- TRANSPARENTNÉ (PRE DOZOROVÝ ÚRAD A FYZICKÚ OSOBU, KTOREJ DÁTA SA SPRACOVÁVAJÚ)
- DOKLADOVATEĽNÉ (PRO DOZOROVÝ ÚRAD)
- V SÚLADE S GDPR, ALE TIEŽ ĎALŠÍMI ZÁKONMI (ZÁKONNÍK PRÁCE, ZÁKONY O ZDRAVOTNOM, SOCIÁLNO, DÔCHODKOVOM ZABEZPEČENÍ A ĎALŠÍMI POISTENIAM, KYBERNETICKEJ BEZPEČNOSTI, ANTISPAMOVÝM ATĎ.)
- MUSIA BYŤ POKRYTÍ VŠETCI DODÁVATELIA– MZDOVÁ UČTÁREŇ, PRÁVNE PORADENSTVO, PERSONÁLNE AGENTÚRY, EXTERNE SPOLUPRACUJÚCI ŠPECIALISTI, KTORÍ MAJÚ PRÍSTUP K OS. ÚDAJOM,....





ČO IMPLEMENTÁCIA PREDSTAVUJE?

- UVEDENIE INTERNÉHO A EXTERNÉHO SPRACOVANIA OS. ÚDAJOV DO SÚLADU S GDPR NARIADENÍ
 - NASTAVENIE ORGANIZAČNÝCH OPATRENÍ, AKTUALIZÁCIA VNÚTORNEJ PREDPISOVEJ BÁZY
 - PROCESNÉ ÚPRAVY RIADIACE SPRACOVÁVANIE A POVINNOSTI
 - NASTAVENIE SPRACOVÁVANIA POŽIADAVIEK OSÔB , KTORÝCH OS. ÚDAJE SA SPRACOVÁVAJÚ
 - POPIS A REALIZÁCIA ÚPRAV INFORMAČNÝCH SYSTÉMOV
 - ZMLUVNÉ A ORGANIZAČNÉ POKRYTIE EXT. SPRACOVATEĽOV, DODÁVATEĽOV APOD.
 - SPRACOVANIE REGISTRA OS. ÚDAJOV, REGISTRA ÚČELOV SPRACOVANIA ATĎ.
 - USKUTOČNENIE BALANČNÝCH TESTOV A POVINNÝCH POSÚDENÍ VPLYVOV NA DOPAD PRÁV OSÔB
 - ZABEZPEČENIE DOKLADOVATEĽNOSTI SÚLADU VOČI DOZOROVÉMU ÚRADU
- ĎALŠIE ...





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
- FINÁLNY AUDIT





AKO DLHO IMPLEMENTÁCIA PREBIEHA

- PODĽA VEĽKOSTI A TYPU ORGANIZÁCIE
- PODĽA TYPU PODNIKANIA– NAPR. PRI FIRMÁCH B2B JE TO KRATŠIA DOBA AKO PRI B2C
- OD 1 MESIACA VO FIRME S NIEKOĽKÝMI ZÁKAZNÍKMI AŽ DO NIEKOĽKO 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 POPIŠUJÚCÍ KONKRÉTNU IMPLEMENTÁCIU V ORGANIZÁCII VYCHÁDZAJÚCI Z NASLEDUJÚCICH 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 APLIKÁCIÍ, REGISTER DODÁVATEĽOV (V ROZSAHU NEVYHNUTNOM PRE IMPLEMENTÁCIU GDPR A PODĽA KONKRÉTNEJ SITUÁCIE V ORGANIZÁCII)
- **FINÁLNY AUDIT**



*Mega***LAN**



Ďakujeme za pozornosť