Влијанието на новата Општа регулатива за заштита на личните податоци врз работата на контролорите од областа на ревизијата во Република Македонија

Дирекција за заштита на личните податоци

GDPR (Општа регулатива за заштита на личните податоци)

- Европскиот парламент и Советот на 27 април 2016 година ја усвоија Општа регулатива
- Ќе започне да се применува од 25 мај 2018 година
- Се воведуваат новини и се модернизираат веќе постојните решенија во Директивата 95/46

GDPR и Република Македонија

- Изработен е целосно нов Закон за заштита на личните податоци, кој е во согласност со новата GDPR

- Ова значи:
  - Нови дефиниции
  - Нови дополнителни начела и принципи
  - Нови обврски за контролорите и обработувачите
  - Засилено значење и улога на офицерите за заштита на личните податоци

GDPR (НОВИ) ДЕФИНИЦИИ

- „Профилирање“ - секоја форма на автоматска обработка на лични податоци, која се состои од користење на лични податоци за оценување на одредени лични аспекти поврзани со физичкото лице, а особено за анализа или предвидување на аспекти кои се однесуваат на извршување на професионалните обврски на тоа физичко лице, неговата економска состојба, здравје, лични преференции, интереси, сигурност, однесување, локација или движење
- „Псевдонимизација“ - обработка на личните податоци на таков начин што личните податоци не можат повеќе да се поврзат со одреден субјект на лични податоци без да се користат дополнителни информации, под услов таквите дополнителни информации да се чуваат одделно и да подлежат на технички и организациски мерки со кои ќе се обезбеди дека личните податоци не се поврзани со идентификувано физичко лице или физичко лице кое може да се идентификува

GDPR (НОВИ) ДЕФИНИЦИИ

- „Генетски податоци“ - лични податоци поврзани со генетските карактеристики на физичкото лице кои се наследени или стекнати, а кои откриваат единствена информација за неговата физиологија или здравје, која особено се добива со анализа на биолошки примерок од тоа физичко лице
- „Биометриски податоци“ се лични податоци кои се добиваат преку специфична техничка обработка на физичките и физиолошките карактеристики на физичкото лице или карактеристики на неговото однесување, а преку кои се одобрува или потврдува единствената идентификација на физичкото лице

GDPR (НОВИ) ДЕФИНИЦИИ

- „Директен маркетинг“ е секој вид на комуникација остварена на било кој начин со цел испраќање на рекламен, маркетиншки или пропаганден материјал која е насочена директно до одреден субјект на личните податоци

Начела и принципи – законитост на обработката

Обработката е законска, само ако и до оној степен доколку е исполнет најмалку еден од следните услови:

- субјектот на лични податоци дал согласност за обработка на неговите лични податоци за една или повеќе конкретни цели;
- обработката е потребна за исполнување на договор каде субјектот на лични податоци е договорна страна, или за да се преземат активности на барање на субјектот на лични податоци пред неговото пристапување кон договорот;
- обработката е потребна за исполнување на законска обврска на контролорот;
- обработката е потребна за заштита на суштинските интереси на субјектот на лични податоци или на друго физичко лице;
- обработката е потребна за извршување на работи од јавен интерес или при вршење на службено овластување на контролорот;
- обработката е потребна за целите на легитимните интереси на контролорот или на трето лице, освен кога таквите интереси преовладуваат над интересите или основните права и слободи на субјектот на лични податоци коишто бараат заштита на личните податоци, особено кога субјектот на личните податоци е дете

Право да се биде заборавен – ново право на субјектот на личните податоци

Субјектот на личните податоци има право да побара од контролорот да ги избрише неговите лични податоци без непотребно одлагање при што контролорот има обврска да ги избрише личните податоци ако е исполнет еден од следните услови:

- личните податоци повеќе не се потребни за целите за кои биле собрани или обработени на друг начин;
- субјектот на личните податоци ја повлекува својата согласност врз која се заснова обработката на податоците и ако не постои друга законска основа за обработката;
- субјектот на личните податоци поднесе приговор на обработката при што не постојат преовладувачки легитимни цели за обработката;
- личните податоци биле незаконски обработени;
- личните податоци треба да бидат избришани со цел почитување на обврска утврдена со закон која се однесува на контролорот;
- личните податоци биле собрани во врска со понудата на услуги на информатичко општество.

Право да се биде заборавен – ново право на субјектот на личните податоци

Кога контролорот ги објавил јавно личните податоци и е должен да ги избрише личните податоци, земајќи ги предвид достапната технологија и трошоците на спроведувањето, тој презема разумни чекори, вклучувајќи технички мерки за да ги извести другите контролори кои ги обработуваат личните податоци дека субјектот на личните податоци побарал бришење на сите линкови или копии или репродукции на личните податоци од страна на тие контролори.

Предизвици за контролорите и обработувачите

- Безбедност на обработката на личните податоци
- Известување за нарушување на безбедноста на личните податоци
- Известување на субјектот на личните податоци за нарушување на безбедноста на личните податоци
- Проценка на влијанието на заштитата на личните податоци и претходна консултација
- Определување на офицер за заштита на личните податоци
- Кодекси на однесување и сертификација

Privacy by Default and Privacy by Design

- Техничката и интегрирана заштита на личните податоци (data protection by design and by default), е една од новите мерки кои се воведуваат како задолжителни за контролорите и обработувачите на личните податоци. Имено, согласно оваа мерка, земајќи ги предвид најновите технолошки достигнувања, трошоците за спроведување, природата, обемот, контекстот и целите на обработката, како и ризиците со различна веројатност и сериозноста на правата и слободите на физичките лица кои произлегуваат од обработката, контролорот ги има следните обврски:
- - во моментот на дефинирање на средствата за обработка, како и во моментот на самата обработка, да примени, односно применува соодветни технички и организациски мерки со кои ќе се обезбеди ефикасно спроведување на начелата за заштита на личните податоци, како што се на пример псевдонимизацијата и сведувањето на минимален обем на податоците (data minimization);
- - да ги примени сите потребни заштитни мерки во процесот на обработката, со цел за да се исполнат условите за законита обработка на личните податоци и воедно да се обезбеди заштита на правата на субјектите на личните податоци.

Privacy by Default and Privacy by Design

- Согласно оваа мерка, контролорот треба да ги примени сите технички и организациски мерки со кои се обезбедува интегрирано (by default), односно на ниво на целиот информациски систем на контролорот, дека се обработуваат само оние лични податоци кои се неопходни за секоја посебна цел на обработката. Оваа обврска се однесува на количеството на собрани лични податоци, опсегот на нивната обработка, рокот на чување и нивната достапност. Воедно, оваа мерка треба да обезбеди дека интегрираните лични податоци без индивидуална интервенција нема да можат да бидат автоматски достапни за неограничен број на физички лица.

Data Protection Impact Assessment

- Согласно оваа контролна мерка, кога при користење на нови технологии за некој вид на обработка на личните податоци, земајќи ги предвид природата, обемот, контекстот и целите на обработката, постои веројатност истата да предизвика висок ризик за правата и слободите на физичките лица, пред да биде извршена обработката, контролорот има обврска да изврши проценка на влијанието на предвидените операции на обработката во однос на заштитата на личните податоци (Data Protection Impact Assessment - ДПИА).

Data Protection Impact Assessment

- ДПИА треба да се врши најмалку во следните случаи:
- во случај на систематска и сеопфатна оценка на личните аспекти кои се поврзани со физички лица, која се заснова на автоматска обработка, вклучувајќи и профилирање, а врз основа на која се донесуваат одлуки кои произведуваат правно дејство во врска со физичкото лице или значително влијаат на физичкото лице;
- во случај на обемна обработка на посебните категории на лични податоци или на лични податоци поврзани со казнени осуди и казнени дела; или
- во случај на систематско набљудување на јавно достапни простори во големи размери.

Известување за нарушување на безбедноста на личните податоци

- Data breach notification
- До ДЗЛП
- До субјектите на личните податоци

- Не е потребно во случај кога контролорот применил ТОМ со кои се гарантира заштитата на личните податоци (криптирање)

Accountability – демонстрирање на усогласеност

- Кодекси на однесување
- Сертификација
- Внатрешни контроли
- DPIA и Privacy by default and by desgn

Ви благодарам на вниманието!