ОПШТА РЕГУЛАТИВА ЗА ЗАШТИТА НА ПОДАТОЦИ
(GENERAL DATA PROTECTION REGULATION – GDPR)

Директивата чија законска примена во ЕУ започнува на 25.05.2018 година, е најдобра пракса со организациски, безбедносни и технички мерки за заштита на приватноста на лицата преку заштита на обработката на лични податоци и информации кои се однесуваат на лицата, чија безбедност (или некое друго право) може да биде нарушена во случај на нивна злоупотреба.

GDPR се занимава со прашања поврзани со заштита на приватни информации и предвидува низа мерки за заштита кои организацијата или деловниот систем мора да ги усвои, со цел да ги исполни минималните правила (пропишани со Уредбата) за кои се верува дека значително ја обезбедува и зачувува приватноста на личните податоци на вработените и корисниците на услуги или клиентите на компанијата, односно корисниците на јавни и државни услуги.

Под приватни податоци се подразбираат податоци за идентитетот на лицата, или податоци од кои може еднозначно да се утврди идентитетот на лицето, политичката и сексуалната ориентација, расата, но и податоци како што се, историја на пребарувањето, мета податоци на датотеки создадени од одредена личност што можат да го откријат идентитетот, здравствената и имотната состојба, движењата, навиките и други лични податоци чие објавување или злоупотреба можат да го загрозат лицето.

GDPR се применува само на лични податоци, што ги вклучува и сите уникатни идентификатори и предвидува псевдонимизација на податоците за да се избегне можноста за злоупотреба. **GDPR предвидува имплементација на разумни мерки** (безбедносни, технички и организациски мерки) **за заштита на приватноста. GDPR не се однесува само на податоци и управување со истите, туку и на деловни процеси кои ги обработуваат податоците.** Во оваа смисла, GDPR предвидува трансфер на обврски; имено, за организациите кои прават аутсорсинг на дел од работата, тие самите се одговорни за оние на кои им ја пренесуваат работата.

Компаниите кои во голема мера вршат системска обработка или мониторинг на личните податоци, мора на многу високо ниво да именуваат службеник за заштита на податоци **(Data**

Protection Officer – DPO)**. **DPO** е одговорен за усогласување на работата на компанијата со GDPR. Во случај кога ефикасна компанија не ги почитува правилата или не е усогласена со GDPR, тогаш правните последици можат да вклучат казна до 20 милиони евра или 4% од годишниот промет.

Основни чекори за примена на GDPR во една организација се следните:

- Подигнување на свеста за GDPR и другите законски, оргнизациски и безбедносни промени кои ги донесува оваа Регулатива.
- Проверка на податоците кои се чуваат и употребуваат во организацијата.
- Запознавање на вработените со доверливоста на информации.
- Дефинирање на индивидуалните права – процедурите мора да ги покриваат сите индивидуални права (право на бришење податоци или давање на податоци во електронска форма).
- Усогласување со правните основи.
- Дефинирање на процедури со кои вработените се запознаени и се согласуваат. Вработените мора да бидат запознаени со процедурите за тоа како ќе се постапува и врши усогласување со нивните лични податоци и записи.
- Дефинирање на процедури за постапување со податоци кои се однесуваат на деца и малолетни лица, и добивање согласност од родител / старател за истите.
- Дефинирање на процедури кои се поврзани со нарушување на безбедноста, истекување на податоци и информации и нивна злоупотреба. Во рамките на овој чекор ќе се дефинираат соодветни процедури за откривање, известување и истрага.
- Дефинирање на стратегија за заштита на податоци преку дизајн и проценка на влијанието на мерките за заштита на податоците.
- Дефинирање на одговорности и описи на работно место за службеникот за заштита на личните податоци – DPO (Data protection Officer) што го предвидува регулативата.
- Доколку, компанијата работи во повеќе од една земја-членка на ЕУ, тогаш GDPR предвидува и супервизор за безбедност.

GDPR

General Data Protection Regulation
Општа уредба за заштита на лични податоци

- **GDPR Practitioner (1 ден)**
- **Data Protection Officer – DPO (2 дена)**