МЕТАМОРФОЗИС
Фондација за интернет и општество

Препораки за нацрт-Националната ИКТ стратегија 2021-2025 и придружниот Акциски план поврзани со правото на приватност

(препораките се дадени во контекст на спроведување на Закон за заштита на личните податоци (Сл.весник на РСМ бр.42/20) и Општата регулатива за заштита на личните податоци (GDPR-General Data Protection Regulation 2016/679)

- Во процесот на зајакнување на ИТ капацитетите на институциите, освен ИТ професионалците, клучен човечки ресурс кој треба сериозно да се планира е и Офицерот за заштита на личните податоци. Улогата на Офицерот за заштита на личните податоци е издигната на повисоко ниво каде стручноста и независноста се на прво место. За да обебзедат ефикасност во исполнувањето на обврските, институциите се должни да обезбедат дека Офицерот за заштита на личните податоци на соодветен начин и навремено е вклучен во сите прашања поврзани со заштитата на личните податоци и да му дадат поддршка при извршувањето на работите, обезбедувајќи му ги сите неопходни ресурси и пристап до личните податоци и операциите на обработка.

- При дефинирањето на инфраструктурата на централниот безбеден податочен центар, особено во делот на преземањето на сите апликации на сите министерства, агенции, институции, универзитети и болници, треба да се има предвид дека голем дел од постоечките апликации не ги имаат вградено начелата за заштита на личните податоци. Секоја институција која има апликација преку која се обработуваат лични податоци треба истата да ја анализира, оцени и задолжително да ги усогласи нејзините функционалности со Законот за заштита на личните податоци пред воопшто да ја предаде во податочниот центар. Неусогласени збирки на лични податоци, апликации и останати е-алатки можат само дополнително да го ослабнат системот за безбедност и заштита на личните податоци, а со тоа да ја доведат во прашање и безбедноста на самиот централен податочен центар.

- Постои суштинска разлика помеѓу е-услугите на институциите кои претставуваат алтернативен начин за добивање на услугата (а не доплнителна услуга која граѓаните не би можеле инаку да ја добијат) и оние услуги кои се единствено достапни на граѓаните на електронски начин (и истите граѓаните не можат да ги добијат на поинаков начин). Ова е клучно прашање кое задолжително мора да се земе предвид во централизирањето на испораката на е-услуги. Кај услугите кои се единствено достапни на граѓаните на електронски начин, принципите за „само еднаш“ и избор на канал ќе мора да се ревидираат и да се преоцени нивната примена.

- Носењето на комуникациска стратегија и планирањето на промотивните активности не смее да биде форсирано пред претходно да биде проверено дали постоечките е-услуги се поткрепени со Политики за приватност, дали се испочитувани сите начела за заштита на приватноста при обезбедувањето на е-услугата и дали институциите имаат дефинирано начин и канали по кои граѓаните можат да побараат остварување на нивното право на приватност.

- Владата треба да се осигура дека работата на секое министерство, орган во состав, институција, јавно претпријатие кое нуди е-услуги е усогласена со Законот за заштита на личните податоци. Ова особено заради фактот што принципот на Безбедност по дизајн се однесува на нови услуги, алатки, апликации, а не на постоечките за кои е очекувано да бидат редефинирани согласно начелата на Законот за заштита на личните податоци.

- Владата треба да осигура дека секоја институција која нуди е-услуги ги почитува принципите на „законитост, правичност и транспарентност“; „ограничување на целите“; „минимален обем на податоци“; „точност“; „ограничување на рокот на чување“; „интегритет и доверливост“ и „отчетност“.

- Во контекст на воспоставување на Центар за побезбеден интернет за деца, Владата треба да го поддржи процесот на транспонирање на Директива (ЕУ) 2016/680 на Европскиот парламент и Советот за заштита на физичките лица во однос на обработката на личните податоци од страна на надлежните тела за цели на спречување, истрага, откривање или гонење на кривичните дела или за извршување на кривичните санкции и за слободното движење на овие податоци со која се обезбедува користење на технолошки средства од страна на полицијата кои не се инвазивни по приватноста. Оваа директива е вториот клучен пропис, покрај Општата регулатива за заштита на личните податоци (General Data Protection Regulation - GDPR) во областа на заштитата на личните податоци која треба да биде дел од националното законодавство.

- При креирањето на нови е-услуги или алатки, особено за услуги за чие обезбедување нема законски пропишана процедура (како што се на пример, СтопКорона, вакцинација.мк, МОЈ ДДВ), Владата треба да ги поддржи институциите во процесот на спроведување на анализа и проценка на влијанието по приватноста како задолжителен прв чекор пред воопшто да се одлучи да се креира самата е-услуга или алатка.

- Односот помеѓу Владата и останатите субјекти треба да биде јасно дефиниран и да се знае кој субјект во кој момент се јавува во улога на обработувач на личните податоци, корисник на личните податоци или трета страна. Овој однос задолжително мора да се регулира со посебни договори помеѓу институциите, а кој се однесува исклучиво на обезбедувањето на мерките за заштита на личните податоци.

- Владата треба да донесе методологија за детекција, пријавување и санирање на безбедносни инциденти поврзани со нарушувањето на безбедноста на личните податоци на граѓаните при користењето на е-услуги или алатки. При тоа, повторен пристап до податоците предмет на инцидентот треба да биде обезбеден без исклучок.

- Агенцијата за заштита на личните податоци (АЗЛП) треба да биде активно вклучена во спроведувањето на стратегијата за ИКТ. Освен како ресурсен центар на знаења и практики, АЗЛП во голем број од активностите ќе треба да даде свое мислење, одобрување и насоки, па затоа нивната инволвираност е суштинска за да се обезбеди процес кој ќе го поддржи спорведувањето на Законот за заштита на личните податоци во секој аспект.