Бр. 03-355/1

26.12.2018 година

Скопје

До:

**Министерство за правда на РМ**

Предмет: **Коментари и предлози за унапредување на Предлог на Закон за заштита на личните податоци**

Почитувани,

Комисијата за информативна сигурност при Македонската Банкарска Асоцијација одржа повеќе работни состаноци со цел разгледување на Предлог на Законот за заштита на личните податоци од кои произлегоа подолунаведените коментари и предлози за унапредување на Законот.

Најпрво, упатуваме на постоење на неколку позначајни забелешки кои би претставувале значајна пречка при неговата примена и општа прифатеност. Имено потребно е пред се:

1. Усогласување на други закони за да не бидат во контрадикторност со овој закон (на пример Закон за електронска трговија, Закон за празници, Закон за архивско работење во делот- Рок на чување на лични податоци).
2. Со овој Закон се предвидуваат прекршочни одредби со кои се предвидуваат глоби со значително големи износи кои се несразмерни со можната загуба за општеството како и споредбено со други глоби предвидени во други закони.
3. Дирекцијата за заштита на лични податоци треба да изготви подзаконски акти кои во целост би го дефинирале Законот и неговата примена.
4. Потребни се зачестени организирани презентации за дискуција со јавниот и приватен сектор со цел подобро разбирање на законските одредби и нивна конкретна практична примена.

**Предлог измени и дополнувања**

**Член 4 – Дефиниции**

# 1.Личен податок –Дефиниција

Забелешка – **Податоци за локација** ако се мисли на IP адреса не би требало да се третира како личен податок со оглед на фактот дека е јавен податок. **Податоци за локација и мрежен идентификатор** се составни делови од ревизорски траги, не треба да се сметаат за лични податоци.

# Точка 5 – Псевдонимизација - Дефиниција

Терминот е нејасен, неупотреблив и дава можност на физичките лица при аплицирање на кредит или било каква друга услуга да се употребува што би значело комплетно нарушување на банкарските системи. Доколку пак компанијата (Контролор) по одреден друг меѓународен стандард треба да го обработува се создава дополнителна работа за негово чување од технички аспект. Исто така овој поим се споменува и во член 29 и наметнува **Прашање ДАЛИ** е задолжително да се овозможи идентификација на клиентите и вработените со употреба на **псевдоними**? Дали согласно член 36 псевдонимизацијата е задолжителна мерка за безбедност на податоците?

# Точка 11 – Согласноста – Дефиниција

Бидејки не е дефинирана согласноста во смисла на Формата (писмена/усна) **Се предлага** во дефиницијата да се допише дека Согласноста треба да биде дадена во форма која ќе овозможи ревизорска трага. Исто така доколку не се прецизира дефиницијата не се води сметка за согласноста која се дава за чување на личните податоци при поврзување на физичкиот идентитет со електронскиот идентитет на субјектите.

#  Точка 13 – Посебни категории на лични податоци – Дефиниција

Законот за празници на РМ прави двојба во примената на одредбите на: граѓани од православна вероисповест, католичка, муслиманска; па оттука и обработката на верата како личен податок не треба да биде во делот на посебни категории на лични податоци.

# Член 6 – Став (2)

Комуникацијата помеѓу Агенцијата и странките треба да биде официјална што би значело дека усната комуникација е неприфатлива, имено истата е тешко докажлива во судски постапки и се смета за правно несигурна. Во оваа насока комуникацијата треба да биде во пишана или во електронска форма.

# Член 7 – Став (1)

Да се дополни со: во случај на писмено барање од Агенцијата или кога Агенцијата ќе поведе постапка за испитување и проверување.

**Член 10 – Став (4)**

Тоа што е наведено во Препорака CM/Rec (2018)2 на Комитетот на министри до земјите-членки за улогите и обврските на интернет посредниците не треба да се цитира, односно да се повикува во текст на закон и воедно дефинирање на мерки на демократско општество не е место во овој закон.

# Член 11 – Услови на согласност

Потребно е дообработка и дообјаснување на овој член поврзано со Условите на Согласност, а во корелација со Дефиницијата за Согласност. Ова е од суштинско значење заради поставување и докажување дека Согласноста е дадена доброволно.

# Член 11 – Став (4)

# Потребно е објаснување од која институција / тело ќе се врши проценка дека согласноста е дадена доброволно и во која постапка?

**Член 16 - Став (4)** - да се брише – Образложение

Ако контролорот не превземе мерки по барањето на субјектот на лични податоци, секако нема да пристапи кон негово информирање за причините за непревземање ниту правно да го поучи.

**Став (7)** - Да се објаснат термините “**стандардизирани икони*”*** и “**Машинско читливи*”.***

***ПРЕДЛОГ*** *-* Да се преформулира цела точка за да биде јасна, разбирлива и применлива.

**Член 17** - Да се дообјаснат Точките 1, 2, 6 од Став (1). Да се дообјасни Точка 6 од став (2). Многу често се употребува терминот „**ако е применливо“**. Како се толкува овој термин во пракса? Став (1), точка 2 да се брише, бидејки контакт информациите на офицерот за заштита на лични податоци се јавно достапни и не треба повторно да се даваат и во моментот на собирањето на личните податоци. Став (2) е преголем товар за банките, во согласност со закон да не се прави во наведениот обем. Став (2) точка 5 да се брише, едукацијата на граѓаните не е обврска на правните субјекти, подигањето на свеста треба да е една од целите на Агенцијата.

**Член 18 –** При примена во пракса би имало проблем на пример кога станува збор за агенции за наплата на долг, адвокати и извршители. Треба да се размисли или да се направи исклучок субјектот ако сака да се информира да му прати барање на пример по електронска пошта на обработувачот за сите овие работи, да не се разбере дека пред секој разговор треба да биде известен.

**Член 19 – Став (1) - Точка 6 -** Едукацијата за правата поврзани со заштитата на лични податоци треба да е на товар на Агенцијата.

**Член 19 – Став (2) -** Не е јасно дали субјектот на лични податоци треба да биде информиран во случај кога неговите податоци се обработуваат локално во РМ, а по одредено време трансферирани за обработка во трета земја, односно дали тоа информирање е поединечно на секој субјект одделно или со соопштение?

**Член 32 – Став (7)** - Цениме дека секоја компанија треба самостојно да прави Договори т.е. Клаузулните договорања да бидат избор на Компаниите. – Се предлага оваа Точка - Да се брише.

**Член 34 – Став (3)** - Треба да биде наведено на која фреквенција треба да се ажурираат овие евиденции.

**Член 34 – Став (1)** - Во Законот не е дефиниран Поимот “**Овластен Претставник*”***- Дали под овластен претставник се подразбира аутсорсинг компанија? Ако да, тогаш ќе треба да се бара од сите добавувачи на кои им се даваат лични податоци за обработка да го изработат ова. На крајот е споменат офицер, на кој офицер се мисли, дали од банката или од аутсорсинг компанијата?

Исто така и во овој член се употребува изразот “Ако е применливо “.

**Член 37 –** Која е целосходноста на известувањето? Што Агенцијата може да стори при нарушување на безбедноста освен да документира?

**Член 38 – Став (3) – Точка (в) -** Со ова јавно би се обелоденил начинот на кој е вршена заштитата и со тоа уште повеќе би се загрозила безбедноста на личните податоци.

**Член 39 – Став (5)** Со цел да не настане забуна, а воедно и да не се изостави некој од начините на обработка на личните податоци, Агенцијата треба мандаторно да објави листа на видовите на операции на обработка за кои не се бара проценка.

**Член 41 - Став (2), Став (5), Став (6) -** Дали ќе има лиценцирани – сертифицирани офицери и дали е ова задолжително во Законот. Секоја компанија да обезбеди свој вработен кој мора да има сертификат или да склучи договор за услуга со сертифициран офицер за заштита на податоци.

**Член 42 – Став (3) –** Да се усогласи со Законот за работни односи.

**Член 42 - Став (6) –** Да се прецизира. Во компаниите и во пракса се покажува дека Офицерот за заштита врши и други работи – Опис на работно место.

**Член 43 – Став (1)** **– точка (б)** **-** Зборот "ревизија" треба да се замени со "контрола".

**Член 46 и Член 47** **-** Дали сертификационите тела наведени во Член 47, Став (1), се вршителите на надворешните ревизии? Дали сертификацијата се однесува само на овие правни лица?

**Член 51** - Дали задолжителните корпоративни правила се обврзувачки само за правни лица кои се дел од група на правни лица? Дали под група на правни лица се подразбира група во МК или и надвор од МК?

**Член 60 – Став (1)** – Се предлага да се додаде дека за избор на Директор на Агенцијата може да биде лице кое освен образование од областа на правото МОЖЕ да биде и од областа на економијата и ИТ Технологијата. – Не треба ограничување на видот на образование.

**Член 66 – Став (1) - Точка (ж)** – Ако сертификационото тело има јасни инструкции на кој начин се врши сертификација, не е јасна поентата да му се нареди да не издава сертификат. Во ваква ситуација доколку не се следат правилата треба сертификационото тело да биде санкционирано заради несоодветно вршење на својата функција.

**Член 69 – Став (5)** – Зашто Сертификатот за обука на офицер да има важност 2 (две) години. Предлагаме ако треба да се сертифицира тоа да биде без временско ограничување. Со ова се прави финансиско обременување. Исто така во целост ниеден Закон не се менува толку често.

Да се размисли околу препорака за негово следење на новините или посети на обуки но не со обврзувачки карактер. Претставува финансиски терет за компаниите.

**Член 71 – Став (1) -** На кој начин ќе биде дефинирано кога обработката на ЛП ќе предизвикува висок ризик за правата и слободите на физичките лица? Дали ова ќе биде уредено со некакви Упатства или друг подзаконски акт?

**Член 79 –** **Став (1)** - Треба да се додаде дека одобрение не е неопходно во случаи кога со друга законска регулатива е регулирано дека мора да се чува одреден тип на посебен личен податок (како на пример копија од лична карта која содржи биометриски податок – слика).

**Член 79 – Став (4) -** Рокот е искучително долг, дури е и зголемен во однос на претходната верзија. Препорака е истиот да се скрати на 30 дена, бидејќи со долг рок се успорува бизнисот.

**Член 84 - Став (8)** **– Чување на видеозаписи** - Се предлага  зборовите „но не подолго од 30 дена “ да се заменат со „но не подолго од 90 дена“. Со ова се дава можност да се чуваат 35 , 45 дена на пример но не повеќе од 90. Во пракса е докажано дека рокот од 30 дена е  краток. Кога ќе се добие сознание за повреда, при спроведување на истраги и рекламации најчесто видео записот е избришан. Клиентот има обврска 1 месечно да подига извод од сметка, но најчесто  тоа не е случај.

**Член 88 -** Се предлага овој член да се брише Образложение.

Првенствено не се познати Целите на овие налепници. Ова повеќе личи на комерцијална активност отколку на регулаторна. Ќе се наплаќаат налепници на секои две години. Банките имаат голем број на видео камери и би имале солидно голем трошок. По кои цени и колку се реалните трошоци за изработка на налепници? Кај банкоматите информацијата дека истите се под видео надзор оди електронски на самиот екран. Дали покрај ова известување ќе треба и на нив да се лепат и налепници? Тоа во многу ќе ги нагрди банкоматите. На пример во Став (4) не е јасен ставот кога Агенцијата дава свое мислење, пред отпочнување на обработката на податоците или по секоја периодична проценка (на секои 2 год.)? Ако е после секоја преоценка, тоа значи дека на секои 2 год. ќе треба да се менуваат огромен број налепници и да се организира акција за нивно лепење по локациите на банките. Во Став (7) не е јасно за која форма се работи? Дали се мисли на Правилник како и до сега?

Со оваа мерка веќе се нарушува безбедноста на објектот/банкоматот. Сосема е доволно да се даде до знаење дека се врши видео надзор, а не и "означување на камерите". На објектот би требало да има една налепница, а не на секоја камера посебно.

**Член 89** - Што се подразбира под ИРВН - , За која цел служи.

Дали е посебно тело? Дали е развиен софтвер? Комплетно нејасно.

На што се мисли? Дека податоци од просторите на сите институции кои се опфатени со видео надзор (снимки од просторот) ќе се чуваат во Агенцијата? Зошто овие податоци агенцијата има ингеренции да ги даде на било кого за одреден надомест и по кој основ? Дали Став (3) значи дека дека ако некој побара ќе добие пристап со опис на камери? Дополнително што Став (7) налага Агенцијата да има јавно достапен тарифник.

Ова е огромен ризик за безбедноста на сите институции во државата.

**Член 91** **– Став (1) -** Не е јасно што ова точно значи. Според терминологијата корисник може да биде физичко, правно лице или орган на државна управа. До сега банките даваат податоци само на државни органи за истраги. Што доколку физичкото лице побара податоци за негова обработка на кои се гледаат витални делови или безбедносни зони на банката (сефови, благајни, банкомати...)? Со тоа очигледно се нарушува безбедноста.

**Член 99 – Став (1) –** Сметаме дека требало да се направи анализа на предлагачот на Законот за финансиските импликации, а потоа да се предложи казнената политика. Одмерувањето до 2% кај фирмите кои имаат голем годишен приход останува на диспозитив на Агенцијата да одлучува колку % би била глобата, при што не се децидно наведени критериумите според кои тоа би се правело.

**Член 99 – Став (3) –** Зошто за државните органи казната е минимална во однос на правните лица со приватна сопственост? Оваква казнена политика воведува нерамноправност помеѓу државните органи и бизнис заедницата.

***Прекршочни Одредби***

# Член 100, Член 101, 102, 103

Премногу високи и неопределени казни. Да се направи намалување на висините на глобите, особено бришење на % од вкупен годишен приход

Образложение

 Република Македонија не е членка во ЕУ – Ова да биде Аргумент првествено на Агенцијата пред ЕУ.

Дополнително, со ваквата казнена политика на овој закон при услови на драстично различен профит од страна на различни компании може да се случи на компанија за помал прекршок да и биде изречена огромна парична казна, додека на компанија со посериозен прекршок (која континуирано не остварува промет) да и биде изречен минимален прекршок или Агенцијата да нема можност да изрече никаков прекршок бидејќи истиот е директно поврзан со % од вкупен годишен приход.

Дополнително начинот на одмерување на глоба во член 103, во услови на така дефинирани членови 100, 101 и 102, остава простор за различно толкување со што се предизвикува правна несигурност кај компаниите. Овој член би требало да остане во предложениот текст од законот доколку се изменат гореспоменатите членови. Со оглед на тоа што овој Закон веќе претставува навлегување на секојдневните активности на било кој контролор, особено на контролори кои обработуваат голем број на ЛП за голем број субјекти, наведените глоби се превисоки и не соодветствуваат со тежината на прекршоците. Ниту еден Закон кој го уредува работењето на Банките, и воопшто на трговските друштва, во ваква, секојдневна оперативна смисла не подржува казни во овој обем.Глобите се превисоки, да се направи фиксирање на сумите - ова е преголема казна за големи компании.

**Член 114** **- Распоредување**

Треба да се усогласи со Законот за работни односи.

**Член 124** **- Право на супервизорот**

Во Алинеја 1 треба точно да се дефинира на кој начин и какви копии од податоци и во колкав обем смее супервизорот да побара и задржи. Ваков недефиниран член претставува сериозен ризик за истекување на сензитивни податоци токму од страна на супервизорот, вклучително и лични податоци. Треба да се дефинира на какви медиуми и со какви заштитни мерки би биле превземани копиите од страна на супервизорите на Агенцијата и какви мерки ќе се превземат и од кого во случај Агенцијата да ја наруши тајноста на податоците кои се задржани.

**Член 130 - Средства за работа**

Во последната алинеја од Став (2) таксативно да се наведе кои се изворите на други приходи што Агенцијата ќе ги остварува. Тоа не треба да се казните, бидејќи би имало конфликт на интереси и така Агенцијата би имала финансиски мотив да изречува казни.

**Член 134** Рокот за донесување на подзаконските акти да биде 1 година од влегување во сила на законот, за да имаат време контролорите да се  усогласат.

**Член 136**  да се брише. Примената на законот во целина  да биде во рок од 2 години по донесување на истиот.

Комисија за информативна сигурност при Македонската банкарска асоцијација Ви стои на располагање за дополниелно образложување во однос на коментарите и предлозите за унапредување на Предлог на Закон за заштита на личните податоци

# МАКЕДОНСКА БАНКАРСКА АСОЦИЈАЦИЈА

 Комисија за информативна сигурност