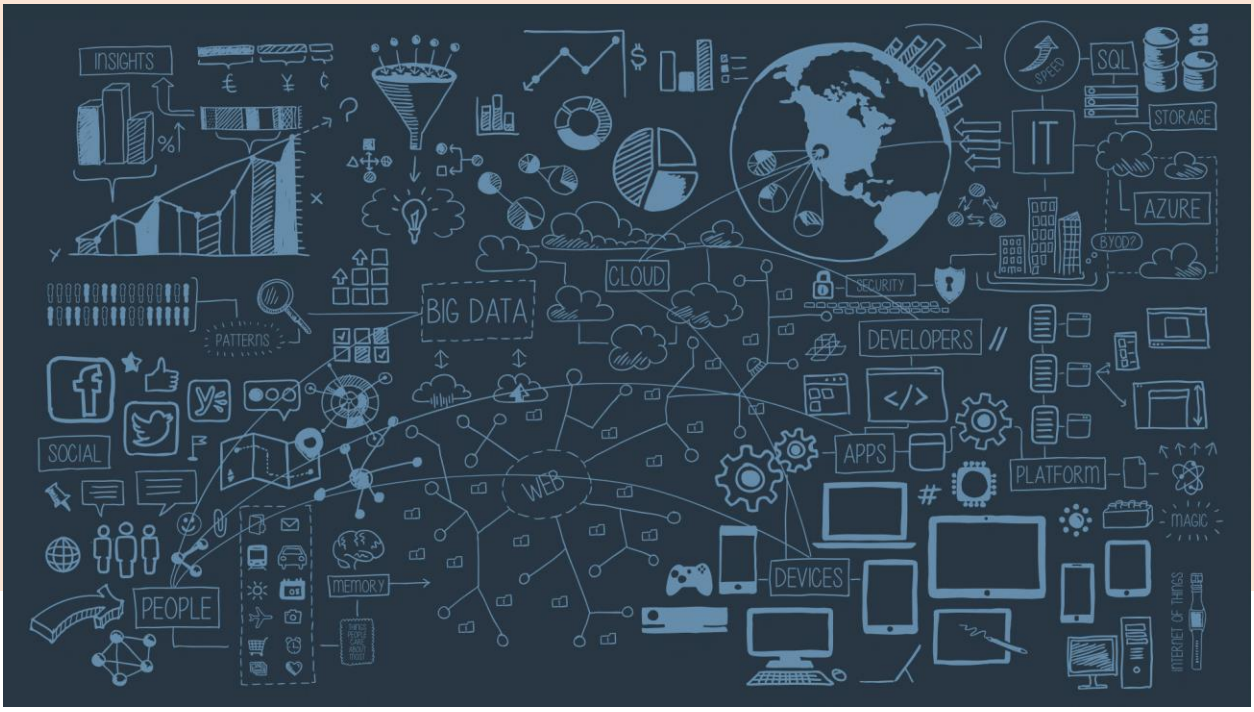
USAID
FROM THE AMERICAN PEOPLE

EPI CENTAR
economy · planning · innovation
Your partner of choice

ПРИРАЧНИК ЗА ИМПЛЕМЕНТАЦИЈА НА ЗАКОНОТ ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ



СТОПАНСКА КОМОРА НА МАКЕДОНИЈА
ECONOMIC CHAMBER OF MACEDONIA

MASIT
ICT Chamber of Commerce

OEMVP

СОЈУЗ НА СТОПАНСКИ КОМОРИ НА МАКЕДОНИЈА
ВОДЕЧКА МАКЕДОНСКА ДЕЛОВНА МРЕЖА

Автори: Емилија Ангеловска, Инфиго ИС ДОО Скопје
Јана Дамевска Атанасова, Инфиго ИС ДОО Скопје

Издавач: Стопанска комора за информатички и комуникациски технологии – МАСИТ

Лектор: Дијана Ристова

Овој прирачник е подготвен од Емилија Ангеловска и Јана Дамевска Атанасова со поддршка на американскиот народ преку Агенцијата на САД за меѓународен развој (УСАИД). Мислењата изразени во оваа публикација „Прирачник за имплементација на Законот за заштита на личните податоци“ им припаѓаат на авторите и не ги изразуваат ставовите на Агенцијата на САД за меѓународен развој или на Владата на Соединетите Американски Држави

Содржина

1. Концепти на обработка на личните податоци 6
2. Принципи на обработка на личните податоци 8
3. Законитост на обработката на личните податоци 11
4. Информирање на субјектот на личните податоци 16
5. Права на субјектите на личните податоци 18
6. Безбедност на личните податоци 22
7. Отчетност (Accountability) 30
8. Пренос на податоци 38
9. Обработка на лични податоци во работни односи 40
10. Активности за надзор и мониторинг 44
11. Директен маркетинг 47
12. Интернет-технологија и комуникации 49
13. Outsourcing 54
14. Регулација и прекршоци 55
15. Заклучок 56
16. Патека до усогласеност со Законот за заштита на личните податоци 57

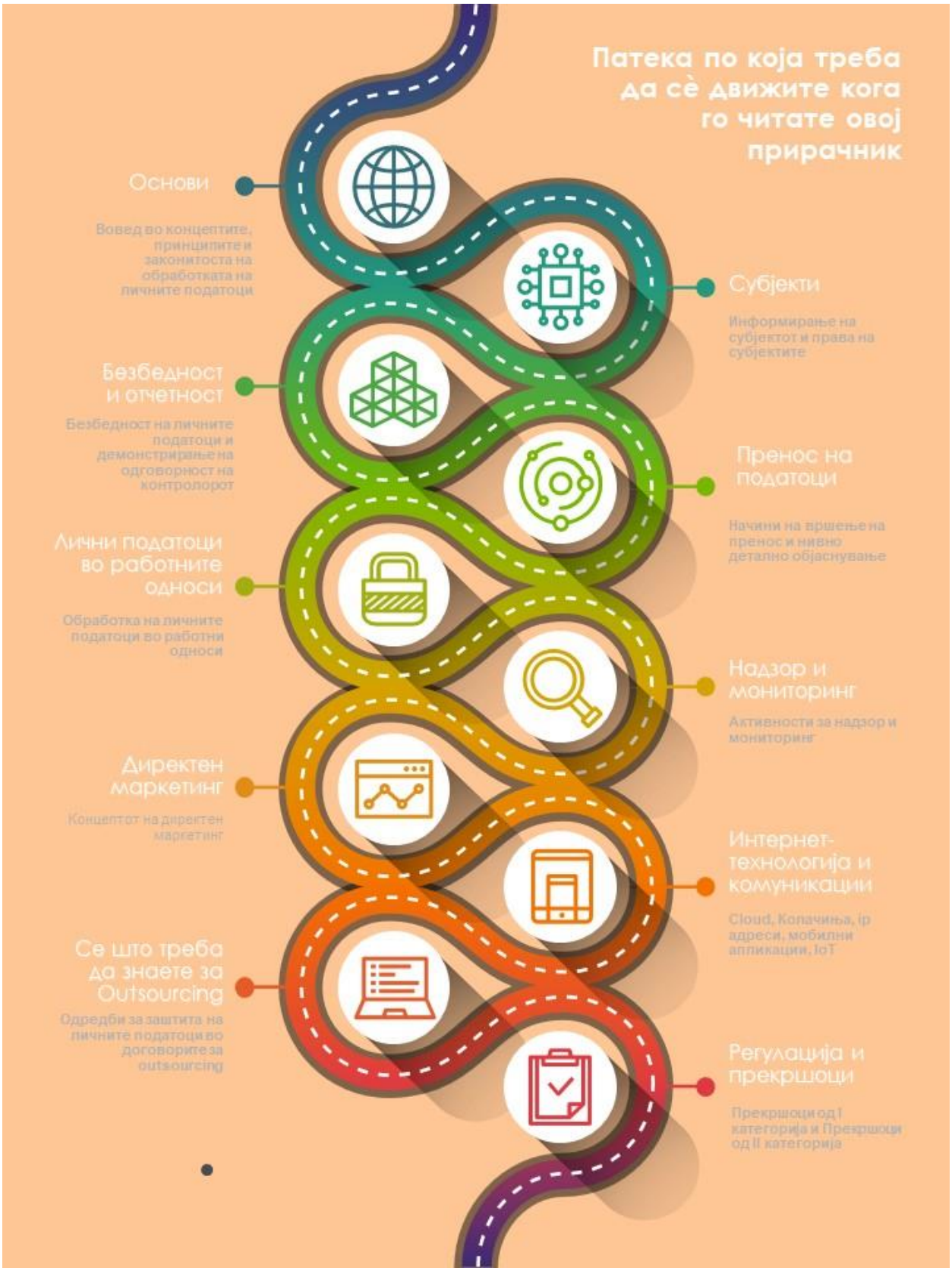
ПРЕДГОВОР

ДРАГИ ЧИТАТЕЛИ,

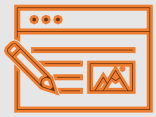
Со донесување Законот за заштита на личните податоци[1], Република Северна Македонија воведе исти правила за заштита на личните податоци како правилата што важат во Европската Унија, предвидени со Општата регулатива за заштита на личните податоци (General Data Protection Regulation 2016/679[2] - GDPR). Имајќи ги предвид предизвиците на компаниите со коишто се соочија при усогласување со GDPR, се претпоставува дека во слична ситуација ќе се најдат домашните компании при усогласување со домашниот Закон за заштита на личните податоци. На дилемите, прашањата и тешкотиите коишто се отвориј на европското тло во контекст на примена на Регулативата, нема да останат имуни ниту македонските компании. Единствената разлика и предност е што од европската пракса може да се извлечат корисни поуки и примери, и со тоа да се дојде до поедноставна и поуспешна имплементација на новите законски обврски и одговорности за заштита на личните податоци.

Целта на овој прирачник е да претставува практичен водич за имплементација на обврските коишто ги наметнува Законот за заштита на личните податоци, притоа користејќи ги европската и домашната регулатива, најдобрите практики, мислења и препораки на европските институции.

[1] „Службен весник на РСМ“ број 42 од 16.2.2020 година
[2] https://eur-lex.europa.eu/eli/reg/2016/679/oj


Патека по која треба да сè движите кога го читате овој прирачник
Основи
Вовед во концептите, принципите и законитоста на обработката на личните податоци
Субјекти
Информирање на субјектот и права на субјектите
Безбедност и отчетност
Безбедност на личните податоци и демонстрирање на одговорност на контролорот
Пренос на податоци
Начини на вршење на пренос и нивно детално објаснување
Лични податоци во работните односи
Обработка на личните податоци во работни односи
Надзор и мониторинг
Активности за надзор и мониторинг
Директен маркетинг
Концептот на директен маркетинг
Интернет-технологија и комуникации
Cloud, Колачиња, ip адреси, мобилни апликации, IoT
Се што треба да знаете за Outsourcing
Одредби за заштита на личните податоци во договорите за outsourcing
Регулација и прекршоци
Прекршоци од I категорија и Прекршоци од II категорија

ПОЧЕТНА ТОЧКА

	Законот за заштита на личните податоци стапи во сила на 25.2.2020 година, со тоа што е предвиден период за усогласување од 18 месеци.
	Законот определува во кои случаи може да се обработуваат лични податоци и кои принципи мора да се почитуваат при тој процес.
	Се промовира обврската на отчетност, односно обврска на компаниите да може да ја докажат својата усогласеност со законот.
	Со законот се зајакнува позицијата на офицерот за заштита на личните податоци.
	Се воведува обврска за компаниите за задолжително известување на Агенцијата за заштита на личните податоци во случај на настан кој може да претставува нарушување на безбедноста на личните податоци.
	Се зголемува висината на прекршоците, и тоа во висина од 2 %, односно 4 % од вкупниот годишен приход на контролорот, односно обработувачот.

Значење на симболите во прирачникот


Предлог за дополнително читање


Позитивен пример


Негативен пример


Препорака за практична примерна

1. Концепти на обработка на личните податоци

Личен податок

Личен податок е секоја информација која се однесува на идентификувано физичко лице или физичко лице кое може да се идентификува...;

Вака дадената дефиниција дава широк спектар на тоа што сè може да претставува личен податок, вклучувајќи име и презиме, ЕМБГ, локација или online идентитет, што ќе предизвика големи промени во технологиите и начините на коишто компаниите обработуваат лични податоци. Се смета дека дури и псевдонимизираните податоци може да се сметаат за лични податоци и да потпаднат под капата на Законот за заштита на личните податоци, во зависност од тоа колку (а не дали) е веројатно да се поврзе псевдонимот со конкретно физичко лице.

Посебна категорија на лични податоци

Личните податоци кои откриваат расно или етничко потекло, политички ставови, верски или филозофски убедувања или членство во синдикални организации, генетски податоци, биометриски податоци, податоци за здравјето, податоци за сексуалниот живот или сексуалната ориентација се сметаат за посебна категорија на лични податоци. Имајќи ја предвид нивната чувствителност, а со тоа и ризиците коишто постојат за субјектите на личните податоци, нивната обработка бара посебни услови и построги мерки за нивна заштита. Личните податоци во врска со осуди за кривични дела не претставуваат посебна категорија на лични податоци, но и за нив, како и за посебната категорија на лични податоци се предвидени дополнителни сигурносни заштитни мерки.[3]

Контролор и обработувач

Контролорот и обработувачот се двата главни столба кои се носители на обврските и одговорностите кои произлегуваат од Законот за заштита на личните податоци.

Контролор → физичко или правно лице кое ги утврдува целите и начинот на обработка на личните податоци.

Обработувач → физичко или правно лице кое ги обработува личните податоци во име на контролорот.

Обработка

Обработка на личните податоци претставува секоја операција којашто се извршува врз личните податоци, сеедно дали автоматски или на друг начин, како на пример собирање, организирање, евидентирање, чување, увид, употреба, копирање, бришење итн. Оваа широка дефиниција речиси и да не остава простор некоја активност да не биде сметана за обработка на лични податоци. Но, за на таа обработка да се применува Законот за заштита на личните податоци, во смисла на неговата материјалната примена,[4] обработката мора да биде целосно или делумно автоматизирана, а доколку не е автоматизирана, да се однесува на лични податоци коишто се дел од постојна збирка на лични

[3] Член 14 од Законот за заштита на личните податоци („Сл. весник на РСМ“ број 42 од 16.2.2020 година)
[4] Член 2 од Законот за заштита на личните податоци („Сл. весник на РСМ“ број 42 од 16.2.2020 година)

податоци[5] или се наменети да бидат дел од збирка на лични податоци.

Субјект на лични податоци

Може да делува изненадувачки фактот дека ниту законот, ниту Општата регулатива за заштита на личните податоци не нудат дефиниција за нешто што е толку значајно како што е субјектот на личните податоци. Во отсуство на јасна дефиниција, од законската дефиниција за тоа што е личен податок, доаѓаме до индиректен заклучок дека субјект на личните податоци е секое „идентификувано физичко лице или физичко лице кое може да се идентификува".[6]

Контролор

Контролорот може да биде физичко или правно лице, орган на државната власт, државен орган или правно лице основано од државата за вршење на јавни овластувања, агенција или друго тело, кое самостојно или заедно со други ги утврдува целите и начинот на обработка на личните податоци, а кога целите и начинот на обработка на личните податоци се утврдени со закон, со истиот закон се определуваат контролорот или посебните критериуми за негово определување.

Обработувач

Обработувач е физичко или правно лице, орган на државната власт, државен орган или правно лице основано од државата за вршење на јавни овластувања, агенција или друго тело кое ги обработува личните податоци во име на контролорот.

Член 4 од Законот за заштита на личните податоци;
Член 4 од Општата регулатива за заштита на личните податоци;

[5] „Збирка на лични податоци е структурирана група лични податоци која е достапна согласно со специфични критериуми, без оглед дали е централизирана или децентрализирана или распространета на функционална или географска основа", член 4 став 1 точка 6 од Законот за заштита на личните податоци („Сл. весник на РСМ" број 42 од 16.2.2020 година)

[6] Член 4 став 1 точка 1 од Законот за заштита на личните податоци („Сл. весник на РСМ" број 42 од 16.2.2020 година)

2. Принципи на обработка на личните податоци

Законот за заштита на личните податоци[7] ги набројува принципите според кои треба да се врши секоја обработка на личните податоци. Овие принципи за обработка на личните податоци се од клучно значење, и го претставуваат темелот на којшто треба да се гради секој систем за заштита на личните податоци. Иако некои од нив беа дефинирани и со претходниот закон[8], со новата законска регулатива се зацврстува нивното значење и важност со тоа што се воведува принципот на отчетност, односно обврска на контролорите да демонстрираат усогласеност со дефинираните принципи.

Законитост, правичност и транспарентност

За обработката на личните податоци да биде во согласност со закон[9], истата најпрво мора да има законски основ, да се врши во мера којашто ќе биде правична и да се врши на транспарентен начин во однос на субјектот на личните податоци чиишто лични податоци се обработуваат.

Законитост

Обработката на личните податоци ќе се смета дека е законита само доколку се врши врз некој од основите определени во членот 10 од законот, а тие се:

Согласност
Исполнување договор
Исполнување законски обврски
Суштински интерес на субјектот на лични податоци
Јавен интерес
Легитимен интерес

Детална анализа за секоја од основите за обработка е дадена во глава 4 од овој прирачник.

Правичност

Следниот принцип што треба да се воспостави, откако ќе се утврди постоењето на законски основ за обработката на личните податоци, е правичноста. Правичната (фер) обработка е поврзана со идејата дека субјектот на личните податоци мора да биде свесен дека неговите лични податоци ќе се обработуваат. Тоа ќе му овозможи да донесе информирана одлука за тоа дали се согласува со таквата обработка и ќе му овозможи исполнување на своите права во однос на заштитата на своите лични податоци.

Пример, компанијата Х дава лични податоци за своите вработени лица на даночните органи, кои пак, согласно даночната регулатива правично ги обработуваат овие лични податоци, без оглед дали субјектите на личните податоци се или не се запознаени со таа обработка.

[7] „Сл. весник на РСМ“ број 42 од 16.2.2020 година
[8] Закон за заштита на личните податоци („Сл. весник на РМ“ бр. 7/2005, 103/2008, 124/2008, 124/2010, 135/2011, 43/2014, 153/2015, 99/2016 и 64/2018)
[9] Закон за заштита на личните податоци („Сл. весник на РСМ“ број 42 од 16.2.2020 година)

Пример: Туристичката агенција АБВ која обработува податоци за однесувањето (behavioral data) на корисниците кои ја користат веб-страницата на агенцијата. Компанијата ги собира овие податоци со користење колачиња и друга технологија за следење со цел да ги анализира преференциите на корисникот додека тој пребарува хотели и авиобилети. Доколку системот е програмиран да донесува автоматизирани одлуки за цената на конкретен аранжман, а и доколку детектира дека корисникот повеќе пати ја посетил веб-страницата пребарувајќи иста конкретна дестинација, зголемување на цената базирано на таа информација се смета за нефер, односно за неправична обработка.

Во пракса најдобро би било да се направи проценка за тоа како обработката влијае на субјектите на личните податоци. Доколку обработката има негативен ефект врз субјектите на личните податоци и таквото влијание не е оправдано, во тој случај обработката не би била фер, односно не би била правична.

Транспарентност

Директно поврзан со принципот на правична обработка е принципот на транспарентност којшто значи дека контролорот мора да биде отворен и јасен кон субјектот на личните податоци при обработка на неговите лични податоци. Наместо досегашното известување на Агенцијата за заштита на личните податоци[10] за збирките на лични податоци коишто се обработуваат, со новите законски правила контролорот има обврска за тоа да ги известува субјектите на личните податоци. Известувањето мора да биде навремено, со користење на јасен и едноставен јазик.[11]

Ограничување на целта

Ограничувањето на целта подразбира дека контролорите може да ги обработуваат личните податоци само за исполнување конкретни, јасни и легитимни цели. Тоа значи дека контролорите најпрво мора да ја идентификуваат конкретната цел за чие исполнување ќе ги обработуваат личните податоци и таа идентификувана конкретна цел да ја претставува рамката во којашто ќе се одвива обработката. Натамошна (секундарна) обработка, за цел поинаква од првичната, може да биде законска само доколку се смета за компатибилна со првичната цел за чие исполнување личните податоци биле првично обработувани.

[10] Со Законот за заштита на личните податоци („Сл. весник на РСМ“ број 42 од 16.2.2020 година) Дирекцијата за заштита на личните податоци се преименува во Агенција за заштита на личните податоци.

[11] Повеќе во член 16 од Законот за заштита на личните податоци („Сл. весник на РСМ“ број 42 од 16.2.2020 година)

Пример: Контролорот нуди фитнес-мобилна апликација на корисници. Конкретната цел за обработка е анализа на личните податоци на корисниците со цел да им се препорачува персонализиран фитнес-план. Натамошната обработка на личните податоци за цел – идентификување на технички грешки на мобилната апликација, ќе се смета за компатибилна со првичната цел, од причина што подобрувањето на мобилната апликација е поврзано со првичната цел.

Пример: Здравствените работници обработуваат лични податоци на пациентите за да ја дијагностицираат и да ја излечат медицинската состојба на нивните пациенти. Споделување на листата со пациенти на осигурителни компании, со цел тие да им ги нудат своите услуги на пациентите, нема да се смета за компатибилна цел со првичната цел за којашто личните податоци се обработуваат.

Минимален обем на податоци

Принципот на обработка на минимален обем на податоци значи дека контролорите ќе ги обработуваат само оние лични податоци кои се соодветни, релевантни и ограничени на она што е неопходно за остварување на целта. Контролорот мора да се осигура дека обработката е навистина неопходна и дека обемот на лични податоци коишто се обработуваат се пропорционални со целта на обработка.

Точност

Принципот на точност подразбира дека контролорот мора да имплементира соодветни мерки за личните податоци коишто ги обработува да бидат точни, и доколку е потребно ажурирани, како и мерки за навремено бришење и коригирање на личните податоци што се неточни или нецелосни.

Ограничување на рокот на чување

Според овој принцип, личните податоци ќе се чуваат во форма која овозможува идентификација на субјектите на личните податоци не подолго од колку што е потребно за исполнување на целите поради кои се врши обработката. Со други зборови, обработката на личните податоци ќе се врши само онолку време колку што е неопходно за да се исполни целта поради која личните податоци се обработувале.

При дефинирање на рокот на чување, контролорот најпрво мора да се осигура дали постојат дефинирани законски рокови за чување на личните податоци, па доколку не, ќе мора да ги дефинира роковите со свои интерни правила.

Интегритет и доверливост

Личните податоци може да се обработуваат само на начин којшто обезбедува соодветно ниво на безбедност на личните податоци со примена на соодветни технички или организациски мерки. За да ги заштитат личните податоци, контролорите треба да имплементираат систем за информациска сигурност којшто е подетално опишан во глава 7 од овој прирачник. При процена и воспоставување на системот за информациска сигурност, честа и добра пракса е тимот да биде составен од правници и технички лица со цел посоодветно дефинирање на стратегиите и политиките на контролорот.

Член 9 од Законот за заштита на личните податоци
Член 5 од Општата регулатива за заштита на личните податоци;

3. Законитост на обработката на личните податоци

Постоењето на законски основ за обработка на личните податоци е директно поврзано со целта поради чие исполнување таа обработка се врши. Контролорот има обврска да дефинира законски основ за секој процес на обработка на личните податоци, а не за личниот податок сам по себе. Обработката на исти лични податоци може да се врши во различни деловни процеси, при што секој деловен процес треба да има соодветен законски основ. Во прилог се детално опишани шесте законски основи за обработка на личните податоци дефинирани во членот 10 од Законот за заштита на личните податоци.[12]

Согласност[13]

Секоја слободно дадена, информирана, конкретна и недвосмислена изразена волја на субјектот на личните податоци, преку изјава или друго јасно потврдно дејствие, а со која се изјавува согласност за обработка на неговите лични податоци претставува законски основ за обработка на личните податоци за конкретната цел за којашто е дадена.

[12] „Службен весник на РСМ“ број 42 од 16.2.2020 година
[13] Член 10, став (1), алинеја 1) од Законот за заштита на личните податоци („Сл. весник на РСМ“ број 42 од 16.2.2020 година)

Слободно дадена согласност

• Го подразбира изборот којшто субјектот на лични податоци го има дали ќе ја даде согласноста или не, како и можноста истата да ја повлече во кое било време. Во проценувањето дали согласноста е слободно дадена особено треба да се земе предвид дали субјектот на личните податоци е условен со извршувањето на договор во којшто тој е договорна страна.

Конкретна согласност

• Подразбира дека субјектот се согласил само за конкретна обработка на неговите лични податоци. Доколку контролорот врши обработка на личните податоци во повеќе процеси, посебна согласност треба да биде дадена за секој процес посебно.

Информирана согласност

• Подразбира дека субјектот на личните податоци ја дал согласноста откако претходно му биле презентирани сите детали за обработката на јазик и во форма коишто се разбирливи за да може соодветно да го процени влијанието коешто обработката може да го има врз него.

Недвосмислена согласност

• Подразбира дека дадената изјава или потврдното дејствие на субјектот не остава простор за сомнеж во неговата намера да се согласи на обработката на неговите лични податоци.

Листа на проверка за контролорите за валидна согласност

✓	Потврдивме дека согласноста е најсоодветниот законски основ за обработка.
✓	Ја побаравме согласноста во текст одделен од општите услови.
✓	Побаравме од субјектите да дадат согласност со потврдна активност.
✓	Не користиме однапред штиклирани квадратчиња или друг тип на претпоставена согласност.
✓	Користиме јасен и недвосмислен јазик кој е лесен за разбирање.
✓	Појасниваме зошто ни се потребни личните податоци и што ќе правиме со нив.
✓	Овозможуваме опции за давање согласност за секоја посебна цел и вид на обработка.
✓	Имаме наведено детали за нашата компанија.

✓	Субјектите на личните податоци се известени дека може да ја повлечат согласноста.
✓	Гарантираме дека субјектите на личните податоци може да одбијат да дадат согласност без никакви последици за нив.
✓	Имаме осигурано дека давањето на согласност не е предуслов за никаква услуга.
✓	Доколку нудиме online услуги на деца, ќе бараме согласност само доколку имаме воспоставено мерки за верификација на возраст.

Исполнување договор

Контролорот може да се повика на овој законски основ кога личните податоци ги обработува со цел да го исполни договорот во којшто субјектот на личните податоци е договорна страна. Исто така, овој законски основ е применлив и за обработката како активност којашто ѝ претходи на потпишување договор со субјектот на личните податоци, доколку овие активности се преземат на барање на субјектот.

Исполнување законски обврски

Обработката на личните податоци којашто контролорот ја врши за да исполни одредени законски барања и обврски, ќе се заснова на овој законски основ и ќе се смета за законита.

Суштински интереси на субјектот на личните податоци

Контролорот врши законска обработка на лични податоци доколку таквата обработка е потребна за заштита на суштинските интереси на субјектот на личните податоци или на друго физичко лице. Заштита на суштинските интереси се применува во услови на живот или смрт, или со други зборови овој критериум ќе биде релевантен само во ретки ситуации на опасност. На пример, доколку субјектот на личните податоци е без свест, обработката на неговите лични податоци може да биде неопходна за да му се овозможи итна медицинска помош.

Јавен интерес

Контролорот врши законска обработка на личните податоци доколку обработката е потребна за извршување работи од јавен интерес или за извршување јавно овластување на контролорот кое е утврдено со закон. Она што е особено значајно кај овој законски основ, и за што контролорот треба да биде особено свесен, е законското право на субјектот на приговор на ваквата обработката на неговите лични податоци (за ова право на субјектите на личните податоци, повеќе во точка 6.7 од овој прирачник).

Легитимен интерес[14]

Обработката ќе се смета за законска доколку контролорот има легитимен интерес да ја спроведува, а тој интерес преовладува над интересите и основните слободи и права на субјектот на личните податоци којшто бара заштита на личните податоци. При проценувањето дали легитимниот интерес преовладува над интересите, правата и слободите на субјектот на личните податоци, контролорот треба да ги земе предвид разумните очекувања на субјектот на личните податоци засновани на постоечкиот однос којшто го има со контролорот. Легитимниот интерес може да постои „каде што има релевантен и соодветен однос помеѓу субјектот на личните податоци и контролорот, во ситуации каде што субјектот на личните податоци е клиент или корисник на услугите на контролорот".[15] Пример за обработка на лични податоци заснована на легитимен интерес е обработката којашто се врши со цел спречување на измами во банкарската индустрија (fraud monitoring), а исто така и обработката којашто се врши за да се обезбеди мрежна и информациска сигурност.

Листа на проверка за легитимен интерес

✓	Проверивме и се осигуравме дека легитимниот интерес е најсоодветен законски основ.
✓	Ја разбираме нашата одговорност за заштита на интересите на субјектите на личните податоци.
✓	Ги идентификувавме релевантните легитимни интереси.
✓	Проверивме и се осигуравме дека обработката е неопходна и дека не постои помалку интрузивен начин за постигнување на истата цел.
✓	Спроведовме тест за избалансираност и се осигуравме дека интересите на субјектите на личните податоци не преовладуваат над нашиот легитимен интерес.
✓	Личните податоци ги обработуваме само на начин на којшто субјектите очекуваат.
✓	Не ги обработуваме личните податоци на начин кој на субјектите на личните податоци би им предизвикал штета.
✓	Доколку обработуваме лични податоци на деца, преземаме дополнителни мерки за да ги заштитиме нивните интереси.
✓	Во нашата документација за приватност, вклучени се информации за легитимниот интерес.

[14] Не е применлив за обработка на личните податоци од страна на органите на државната власт при спроведување на нивните надлежности

[15] Recital 47, General Data Protection Regulative 2016/679, https://eur-lex.europa.eu/eli/reg/2016/679/oj

Обработка на посебна категорија на лични податоци

Според Законот за заштита на личните податоци, обработката на посебната категорија на лични податоци кои откриваат расно или етничко потекло, политички ставови, верски или филозофски убедувања, членство во синдикати, како и генетски податоци, биометриски податоци, податоци за здравјето и за сексуалната припадност, е забранета!

Исклучоци од ова правило постои и истите се предвидени во членот 13 од законот.

Контролорот мора да ја определи законската основа за обработка на личните податоци пред започнување со обработката. Важно е да се нагласи значењето на добра проценка за тоа кој основ е применив и документирање на таа одлука. Можно е да се појават ситуации во коишто ќе биде применлив повеќе од еден основ, и во тој случај контролорот мора да разјасни уште пред самата обработка на кој основ ќе се повика.

Пример: Компанија Х одлучува дека обработката на личните податоци ќе ја заснова на согласноста на субјектите на личните податоци. Во текот на активностите, некој од субјектите решава да го оствари своето право и да ја повлече дадената согласност, што за компанијата Х значи дека мора да ја прекине обработката на неговите лични податоци. Компанијата сепак одлучува да ја продолжи обработката на овие лични податоци менувајќи го основот од согласност во легитимниот интерес. Дали постапила правилно? Дури и да постои легитимен интерес, компанијата Х не може да го промени законскиот основ по започнување на обработката. Компанијата Х требала уште пред започнување на обработката, да го информира субјектот на личните податоци дека законски основ за обработка на неговите лични податоци е легитимниот интерес. Наведувајќи го субјектот на личните податоци да верува дека има избор, а таквиот избор не е релевантен, не е правично. Па така, компанијата Х по повлечената согласност, морала да ја прекине натамошната обработка на личните податоци на субјектот кој ја повлекол согласноста.

Листа за проверка за постоење законски основ за обработка

✓	Ги ревидиравме нашите активности за обработка на личните податоци и за која активност определивме соодветна законска основа за обработка.
✓	Проверивме дали обработката е неопходна за исполнување на целта заради која ја вршиме и потврдивме дека не постои друг разумен начин за да ја постигнеме таа цел.
✓	Ја документиравме нашата одлука за тоа која законска основа е применлива за секоја активност.
✓	Во нашата Политика за приватност вклучивме информации за целта на обработката на личните податоци и за законскиот основ за вршење на обработката.
✓ ✓	Во ситуациите кога обработуваме посебна категорија на лични податоци, ги определивме условите во коишто е можна обработка на овие податоци и овој процес е документиран.
✓	Во ситуациите кога обработуваме лични податоци за кривични дела, ги определивме условите во коишто е можна обработка на овие податоци и овој процес е документиран.

Членови 10-15 од Законот за заштита на личните податоци
Членови 6-11 од Општата регулатива за заштита на личните податоци;
Guidelines on consent under GDPR, 28.11.2017, WP29

4. Информирање на субјектот на личните податоци

Информации со кои се запознава субјектот на личните податоци

Принципот на транспарентност, или обврската на контролорот да биде јасен, чесен и отворен за начинот на којшто ги обработува личните податоци, е она што претставува значајна новина којашто се воведува со новиот Закон за заштита на личните податоци. Законските одредби го гарантираат правото на субјектот на личните податоци да добие одредени информации од контролорот, независно дали тие лични податоци контролорот ги добил лично од субјектот или пак од некоја трета страна. Таа разлика е значајна во однос на количината на информации и времето кога овие информации треба да му бидат дадени на субјектот на личните податоци.

Дополнителни информации во специфични ситуации

Без оглед дали личните податоци се добиени директно од субјектот или од трета страна, законот предвидува дополнителни информации коишто, во специфични ситуации, треба да им се предочат на субјектите на личните податоци. Таква ситуација е преносот на личните податоци во трета земја за што контролорот мора да го информира субјектот на личните податоци и да го запознае со детали кои се однесуваат на преносот. Втора таква

ситуација е кога контролорот планира да врши обработка на лични податоци за цели поинакви од целите за коишто првично ги собрал податоците. И трета таква обврска за давање информации постои при одредени нарушувања на безбедноста на личните податоци, кога контролорот е обврзан во соодветен рок да ги извести и субјектите на личните податоци.

Исклучоци од обврската за информирање на субјектот на личните податоци[16]

Контролорот е ослободен од обврската да ги информира субјектите на личните податоци во конкретно дефинирани ситуации, при што повторно се прави разлика во однос на начинот на тоа како се добиени личните податоци.

Доколку личните податоци се добиени директно од субјектот на личните податоци	• Субјектот веќе располага со тие информации.
Доколку личните податоци не се добиени директно од субјектот	• Субјектот веќе располага со тие информации. • Обезбедувањето на тие информации е невозможно или бара несразмерно голем напор.

Членови 16-18 од Законот за заштита на личните податоци
Членови 12-14 од Општата регулатива за заштита на личните податоци; Guidelines on transparency under GDPR, WP29

[16] Член 27 од Законот за заштита на личните податоци („Сл. весник на РСМ“ број 42 од 16.2.2020 година)

5. Права на субјектите на личните податоци

Како што е претходно наведено, принципот на транспарентност е фундаментален принцип на секој систем за заштита на личните податоци. Не може да се осигура правото на приватност на субјектите на личните податоци доколку тие не се соодветно информирани за активностите на контролорот. Во суштина, за остварување на правата на субјектите на личните податоци се тргнува од претпоставката дека субјектите ги имаат сите информации коишто им се потребни со цел да ја разберат природата на обработката.

Овој вид на барања може да претставува значителен административен товар за контролорите, па препорака за контролорите е однапред да ги имаат дефинирано процесите низ коишто ќе се спроведуваат овие барања (т.н. управување со права на субјектите на личните податоци). Контролорите коишто ќе целат кон овозможување примена на правата на субјектите на личните податоци, би требало истите да ги инволвираат во своите процеси со примена на privacy by design и privacy by default.

Право на информираност

Според членовите 17 и 18 од законот, субјектот на личните податоци има право да биде информиран за идентитетот на контролорот, неговите контакт-податоци, целта на обработка, законската основа на обработка и други релевантни информации коишто се неопходни за да осигураат правична и транспарентна обработка на личните податоци.

Право на пристап на субјектот на личните податоци[17]

Правото на пристап на субјектот на личните податоци во одредена смисла е активната страна на медалјонот, додека правото на информираност од членовите 17 и 18 е неговата пасивна страна. Секој субјект на личните податоци може да побара информација од контролорот дали се обработуваат негови лични податоци.

Право на исправка[18]

Со ова право им се овозможува на субјектите на личните податоци да побараат исправка на нивните неточни или нецелосни лични податоци, а контролорот мора да се осигура дека неточните или нецелосните лични податоци се избришани, дополнети или исправени. Освен промена во своите бази со податоци, контролорот за ова барање и промена мора да ги извести и третите страни на коишто им се дадени конкретните лични податоци на користење, за и тие да ги коригираат неточните или нецелосните лични податоци.

[17] Член 19 од Законот за заштита на личните податоци („Сл. весник на РСМ“ број 42 од 16.2.2020 година)
[18] Член 20 од Законот за заштита на личните податоци („Сл. весник на РСМ“ број 42 од 16.2.2020 година)

Право на бришење (Right to be forgotten)[19]

Субјектот на личните податоци има право да побара од контролорот да ги избрише неговите лични податоци, доколку е исполнет некој од следните услови:

- Личните податоци повеќе не се потребни за целите за коишто биле собрани;
- Доколку обработката се засновала на согласност, а субјектот на личните податоци ја повлекол согласноста;
- Субјектот на личните податоци поднел приговор[20] против обработката;
- Личните податоци биле обработувани незаконски;
- Личните податоци треба да бидат избришани како резултат на законска обврска на контролорот;
- Личните податоци биле собрани во врска со понуда на услуги од информатичкото општество на деца.

Доколку контролорот ги објавил јавно личните податоци за коишто е побарано да бидат избришани (на пр. во телефонски именик или на социјални медиуми), мора да преземе разумни мерки за да ги информира сите трети страни коишто во меѓувреме ги преземале личните податоци за да ги обработуваат како контролори, за остварување на правото на субјектот да биде заборавен.

Контролорот може да го одбие барањето на субјектот на личните податоци да биде заборавен, доколку обработката е потребна за остварување на правото на слобода на изразување и информирање, за усогласување на контролорот со законска обврска, или за извршување на работи од јавен интерес меѓу кои и јавното здравство, како и за целите на архивирање од јавен интерес, за научни, историски или статистички истражувања.[21]

Освен промена во своите бази со податоци, контролорот мора за ова барање да ги извести третите страни (корисници) на кои им се дадени на користење конкретните лични податоци.

Право на ограничување на обработката[22]

Субјектот на личните податоци има право да побара ограничување на обработката на неговите лични податоци, доколку:

- Точноста на личните податоци е оспорена од страна на субјектот (обработката ќе биде ограничена додека се провери точноста на податоците);
- Обработката е незаконска, а субјектот се спротивставува личните податоци да се избришат;
- Контролорот нема повеќе потреба од личните податоци од причина што целта за нивната обработка е исполнета, а субјектот бара да се чуваат поради остварување на негови правни барања;

[19] Член 21 од Законот за заштита на личните податоци („Сл. весник на РСМ“ број 42 од 16.2.2020 година)
[20] Член 25 од Законот за заштита на личните податоци („Сл. весник на РСМ“ број 42 од 16.2.2020 година)
[21] Член 21, став (3) од Законот за заштита на личните податоци („Сл. весник на РСМ“ број 42 од 16.2.2020 година)
[22] Член 22 од Законот за заштита на личните податоци („Сл. весник на РСМ“ број 42 од 16.2.2020 година)

- Субјектот на личните податоци поднел приговор за обработката и дури се чека верификација чии интереси преовладуваат (легитимните интереси на контролорот наспроти интересите на субјектот) обработката се ограничува.

Освен промена во своите системи, контролорот мора за ова барање да ги извести третите страни (корисници) на кои им се дадени на користење конкретните лични податоци.

Право на преносливост на личните податоци[23]

Правото на преносливост на личните податоци е новина во регулативата за заштита на личните податоци. Законот му дава право на субјектот на личните податоци да ги добие неговите лични податоци во структуриран, вообичаено користен и машински читлив формат. Исто така, субјектот на личните податоци има право овие лични податоци да ги пренесе на друг контролор, без попречување од страна на контролорот од кого се бара преносливост. Контролорот мора да може да му ги предаде личните податоци на субјектот на личните податоци, или на барање на субјектот, да ги пренесе личните податоци директно на друг контролор доколку е тоа технички возможно. Ова право, субјектот може да го искористи само ако:

- тој му ги има дадено личните податоци на контролорот,
- обработката се врши врз основа на согласност[24] или врз основа на договорна обврска[25] или
- обработката се врши на автоматизиран начин.

Право на приговор[26]

Доколку личните податоците на субјектот се обработуваат врз основа на јавен интерес[27] или легитимен интерес на контролорот[28], вклучувајќи профилирање и директен маркетинг, субјектот има право да поднесе приговор против таквата обработка. Контролорот како одговор на приговорот ќе мора да ја запре обработката, освен ако не докаже дека неговиот легитимен интерес преовладува над интересите, правата и слободите на субјектот на личните податоци.

Она што е специфично за ова право, е дека неговото постоење мора да му се предочи на субјектот на јасен начин, издвоено како информација од останатите информации коишто му се даваат на субјектот на личните податоци (членови 17 и 18 од законот).

[23] Член 24 од Законот за заштита на личните податоци („Сл. весник на РСМ“ број 42 од 16.2.2020 година)
[24] Член 10, став (1), алинеја 1) и член 13, став (2), алинеја 1) од Законот за заштита на личните податоци („Сл. весник на РСМ“ број 42 од 16.2.2020 година)
[25] Член 10 став 1 алинеја 2 од Законот за заштита на личните податоци („Сл. весник на РСМ“ број 42 од 16.2.2020 година)
[26] Член 25 од Законот за заштита на личните податоци („Сл. весник на РСМ“ број 42 од 16.2.2020 година)
[27] Член 10, став (1), алинеја 5) од Законот за заштита на личните податоци („Сл. весник на РСМ“ број 42 од 16.2.2020 година)
[28] Член 10, став (1), алинеја 6) од Законот за заштита на личните податоци („Сл. весник на РСМ“ број 42 од 16.2.2020 година)

Право да не биде предмет на автоматско донесување на одлуки и профилирање[29]

Ова право на субјектот на личните податоци да не биде евалуиран врз основа на автоматска обработка и профилирање на неговите лични податоци е тесно поврзано со правото на приговор. Многу е важно да се нагласи дека ова право се однесува само на оние одлуки кои се засновани исклучиво на автоматска обработка и профилирање, и кои предизвикуваат правни последици или на сличен начин влијаат на субјектот на личните податоци. Контролорот ќе го одбие барањето од субјектот на личните податоци за остварување на ова право, доколку одлуката која е предмет на автоматска обработка или профилирање:

- е потребна за склучување или извршување на договор помеѓу субјектот на личните податоци и контролорот;
- е дозволена со закон којшто се применува во однос на контролорот или
- се заснова на изречна согласност на субјектот на личните податоци.

Ограничувања на правата на субјектите на личните податоци[30]

Правата на субјектите на личните податоци и нивното остварување може да се каже дека се суштина на регулативата за заштитата на личните податоци. Но, во одредени ситуации кои ги предвидува регулативата, овие права на субјектите на личните податоци можат да се ограничат. Таквото ограничување може да се случи само кога претставува неопходна и национална мерка со цел справување со прашања од типот на национална сигурност, јавна безбедност, одбрана и слично[31].

Членови 19 - 26 од Законот за заштита на личните податоци;
Членови 15 – 23 од Општата регулатива за заштита на личните податоци;
Правилник за начинот на известување за нарушување на безбедноста на личните податоци;
Guidelines on automated decision making and profiling for the purposes of GDPR, WP29.

[29] Член 26 од Законот за заштита на личните податоци („Сл. весник на РСМ“ број 42 од 16.2.2020 година)
[30] Член 27 од Законот за заштита на личните податоци („Сл. весник на РСМ“ број 42 од 16.2.2020 година)
[31] Повеќе за ситуациите кога се ограничени правата на субјектите, во член 27 од Законот за заштита на личните податоци („Сл. весник на РСМ“ број 42 од 16.2.2020 година)

6. Безбедност на личните податоци

Безбедноста на личните податоци е прашање кое е многу пошироко од едноставна примена на соодветни технички и организациски мерки. Безбедноста е предуслов за постигнување усогласеност со сите други принципи на обработка на личните податоци. Со други зборови, отсуството на безбедност, освен што само по себе ќе претставува неусогласеност според членот 36 од законот, туку како резултат ќе произведе и други неусогласености со спектарот на обврски од целиот закон.

Принцип на безбедност базиран на анализа на ризици

Контролорот и обработувачот, користејќи пристап базиран на анализа на ризици, ќе преземат соодветни технички и организациски мерки за да обезбедат ниво на безбедност коешто ќе биде соодветно на нивото на ризикот. Ризиците може да бидат случајни и од невнимание, па сè до злонамерни активности, па така и мерките треба да се движат од заштита против комплексни технолошки закани, како што се злонамерни софтвери и DOS-напади, па сè до мерки против невнимание на вработени лица.

Освен ризиците, при избор на соодветни технички и организациски мерки треба да се земат предвид и најновите технолошки достигнувања, трошоците за спроведување, природата, обемот, контекстот и целите на обработката. Преземените мерки, контролорот и обработувачот, треба да ги опишат во евиденцијата на активностите за обработка за секоја операција на обработка посебно (доколку има обврска да води таква евиденција).

Според Правилникот за безбедност на обработката на личните податоци,[32] контролорот и обработувачот, задолжително треба да ги имплементираат најмалку следните мерки:

[32] „Службен весник на РСМ“ број 122 од 12.5.2020 година

Технички мерки (Стандардно ниво)	Технички мерки (Високо ниво)
☐ Автентикација на овластени лица	☐ Управување со лозинки
☐ Обезбедување опрема на која се врши обработка на личните податоци	☐ Сертификација за заштита на личните податоци
☐ Сегрегација на должности и одговорности	☐ Управување со преносливи медиуми
☐ Контрола на пристап до информацискиот систем	☐ Тестирање на информацискиот систем
☐ Обезбедување евиденција за секој пристап (logs)	☐ Сертификациони постапки
☐ Обезбедување на преносливите медиуми	☐ Пренесување на медиуми
☐ Заштита на внатрешната мрежа	☐ Пренесување на личните податоци преку мрежа за електронски комуникации
☐ Обезбедување на серверите	
☐ Обезбедување на веб-страницата	
☐ Обврски и одговорности	
☐ Обезбедување континуитет во работењето	
☐ Начин на архивирање и чување на податоците	
☐ Управување со преносливи медиуми	
☐ Криптирање на личните податоци	
☐ Физичка безбедност	
☐ Контрола на информацискиот систем и инфраструктурата	
☐ Управување со обработувачи	

Организациски мерки (Стандардно ниво)	Организациски мерки (Високо ниво)
☐	☐
☐ Информирање и едуцирање за заштитата на личните податоци	☐ Копирање и умножување документи
☐ Пристап до документите	☐ Пренесување документи
☐ Правило на „чисто биро“	
☐ Чување документи	
☐ Уништување документи	
☐ Начин на чување на документите	

Доверливост и вработени лица

Обврската за безбедност се однесува и на активностите на вработените и на другите овластени лица. Имено, сите лица коишто имаат пристап до личните податоци за време на нивното работење кај контролорот или обработувачот, треба да постапуваат исклучиво според обврска за доверливост. Идејата е дека уште со договорот за вработување овие лица ќе се обврзат дека ќе работат исклучиво во границите на добиените упатства од страна на контролорот или обработувачот и дека нема да ги злоупотребат личните податоци за нивна или за нечија друга потреба и цел.

Однос помеѓу контролорот и обработувачот

Контролорот може да соработува само со оние обработувачи коишто обезбедуваат доволна гаранција за примена на соодветни технички и организациски мерки. Исто така, контролорот мора да обезбеди начин на кој ќе може да докаже дека избрал соодветен обработувач. „Доколку контролорот не може да обезбеди доказ за компетентноста на обработувачот, тогаш обработувачот мора да си оди, или тоа во спротивно би било автоматско прекршување на членот.(н.з. 32)“.[33] Откако контролорот ќе избере соодветен обработувач, мора да се осигура дека на обработувачот ќе му ги делегира сите применливи принципи за обработка на личните податоци. Клучен контролен механизам за тоа е употреба на договор кој ќе ги содржи сите задолжителни елементи дефинирани во ставот 3 на членот 32 од законот.

Она што претставува новина во односот помеѓу контролорот и обработувачот е должноста на обработувачот да му помогне на контролорот да обезбеди усогласување и намалување на ризиците, што подразбира помагање на контролорот за исполнување на законските барања за известувања во случај на нарушување на безбедноста на личните податоци.[34]

[33] Стр. 176 од European Data Protection Law and Practice, IAPP, 2018

[34] Член 32, став (3), алинеја ѓ) од Законот за заштита на личните податоци („Сл. весник на РСМ“ број 42 од 16.2.2020 година)

Известувања при нарушување на безбедност на личните податоци

Членовите 37 и 38 од законот му наметнуваат обврска на контролорот да ја извести Агенцијата за заштита на личните податоци, а во одредени ситуации и засегнатите субјекти на личните податоци, доколку настане нарушување на безбедноста на личните податоци. Со ваквата транспарентност им се помага на контролорите, регулаторите и општеството да ги разберат причините за настаните, овозможувајќи развивање на соодветни активности со кои ќе се намалат ризиците од идни такви настани и намалување на нивното влијание.

Што претставува нарушување на безбедноста на личните податоци?

Според законската дефиниција, нарушувањето на безбедноста на личните податоци претставува настан кој доведува до случајно или незаконски уништување, губење, менување, неовластено откривање или пристап до личните податоци кои се пренесуваат, чуваат или на друг начин обработуваат.[35]

Известување на Агенцијата за заштита на личните податоци

Доколку некој настан се класифицира како нарушување на безбедноста на личните податоци кое претставува[36] ризик за правата и слободите на субјектите на личните податоци, контролорот мора за тоа да ја извести Агенцијата за заштита на личните податоци. Обврската за известување треба да се исполни веднаш, односно не подолго од 72 часа откако контролорот дознал за безбедносниот настан. Од правен и оперативен аспект, грешна би била интерпретација на одредбата дека треба да се избегнува имплементирање мерки за детекција на безбедносни настани, со цел избегнување откривање на безбедносниот настан, а потоа и негово „пријавување". Од оперативен аспект, мерките за детекција на безбедносни настани се неопходни во сите компании, а од правен аспект, немањето на мерки за детекција на нарушување на безбедноста, претставува неусогласеност со принципот на безбедност[37] и го изложува контролорот на правен ризик.

Ако се земе предвид временскиот период потребен за детекција и класификација, како и краткиот рок за известување, препорака за контролорите е да имаат усвоено стратегија за справување со инциденти. Ваквата стратегија добро е да содржи план за справување со инциденти, процедура за справување со инциденти (објаснета чекор по чекор), тим за справување со инциденти и оперативен тим за детекција на инциденти (на пример – security operations center, SOC).

[35] Член 4, став (1), алинеја 12) од Законот за заштита на личните податоци („Сл. весник на РСМ" број 42 од 16.2.2020 година)

[36] Во член 37 став 1 од Законот за заштита на личните податоци е наведено дека обврската на контролорот постои "..., освен ако не постои веројатност нарушувањето на безбедноста... да создаде ризик...", што веројатно претставува несоодветен превод на одредбата од членот 33 од Општата регулатива за заштита на личните податоци каде што е наведено "..., unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons"

[37] Член 9, став (1), алинеја 6) од Законот за заштита на личните податоци („Сл. весник на РСМ" број 42 од 16.2.2020 година)

Известување на субјектите на личните податоци

Во случај на нарушување на безбедноста на личните податоци за кое постои веројатност дека може да има висок ризик за правата и слободите на субјектите на личните податоци, контролорот има обврска за тоа веднаш да ги извести засегнатите субјекти на личните податоци.

Законот нуди исклучоци[38] од оваа обврска на контролорот. Првиот исклучок настанува во случај на преземени соодветни технички и организациски мерки, особено мерки кои ги прават личните податоци неразбирливи, на пример, со нивно енкриптирање. Поинаку кажано, примената на енкрипција има дерегулаторен ефект, бидејќи го ослободува контролорот од обврската за известување. Вториот исклучок настанува кога контролорот применил дополнителни мерки за да спречи појавување висок ризик, што воедно претставува дополнителна причина за добра и квалитетна стратегија за справување со инциденти. Третиот исклучок е делумен и настанува кога за известувањето се бара несразмерен напор од страна на контролорот.

Примери за нарушувања на безбедност на лични податоци

Пример	Известување на АЗЛП	Известување на субјектите на личните податоци
Контролорот чувал бекап на архива на криптирани лични податоци на USB. За време на кражба, USB-то е украдено.	Не.	Не.
Контролорот нуди онлајн услуги. Како резултат на сајбер напад, личните податоци на клиентите се компромитирани.	Да, треба да ја извести Агенцијата, доколку постои веројатност од ризик за правата и слободите на физичките лице.	Да, во зависност од природата на засегнатите лични податоци и доколку постои веројатност од висок ризик за субјектите на личните податоци.
Во e-mail-от за директен маркетинг, примателите се наведени во полињата „to“ или „cc”, откривајќи ги на секој примател e-mail адресите на останатите примателите.	Да, доколку се засегнати голем број на субјекти на лични податоци, или се откриени чувствителни податоци (пр. меил листа на психотерапевт), или постојат други фактори за висок ризик.	Да, во зависност од опсегот и видот на личните податоци и дали постои веројатност од висок ризик за субјектите на личните податоци

[38] Член 38, став (3) од Законот за заштита на личните податоци („Сл. весник на РСМ“ број 42 од 16.2.2020 година)

Елементи на известувањата до Агенцијата и до субјектите на личните податоци

Агенцијата за заштита на личните податоци, како прилози на Правилникот за начинот на известување за нарушување на безбедноста на личните податоци[39] има усвоено обрасци коишто контролорот треба да ги пополни при нарушување на безбедноста на личните податоци и да ги достави до Агенцијата и, доколку е потребно, до субјектите на личните податоци. Со нивното донесување, им се олеснува работата на контролорите од причина што веќе однапред им е дефинирано кои податоци и детали треба да ги достават до Агенцијата и до субјектите на личните податоци (доколку е тоа потребно).

Обезбедување на безбедноста

Во овој дел од Прирачникот ќе бидат дискутирани некои од предизвиците со коишто контролорите и обработувачите би можеле да се соочат за време на усогласување со принципот на безбедност и намалување на ризиците.

Проценка на ризиците

Пред спроведување на самата анализа на ризици, претходно треба да се состави список на процеси во кои се врши обработка на личните податоци, а кои ќе ги опфати, меѓу другото, хардверот, софтверот, комуникациските канали и документите во хартиена форма. Потоа за секој процес на обработка треба да се направи посебна анализа на ризиците која ќе ги опфаќа потенцијалните влијанија и ефекти, изворите на ризик, идентификување на можните закани, постојни или планирани мерки за справување со секој ризик, и оценување на сериозноста и веројатноста од настанување на секој ризик.[40]

Ефективен менаџмент

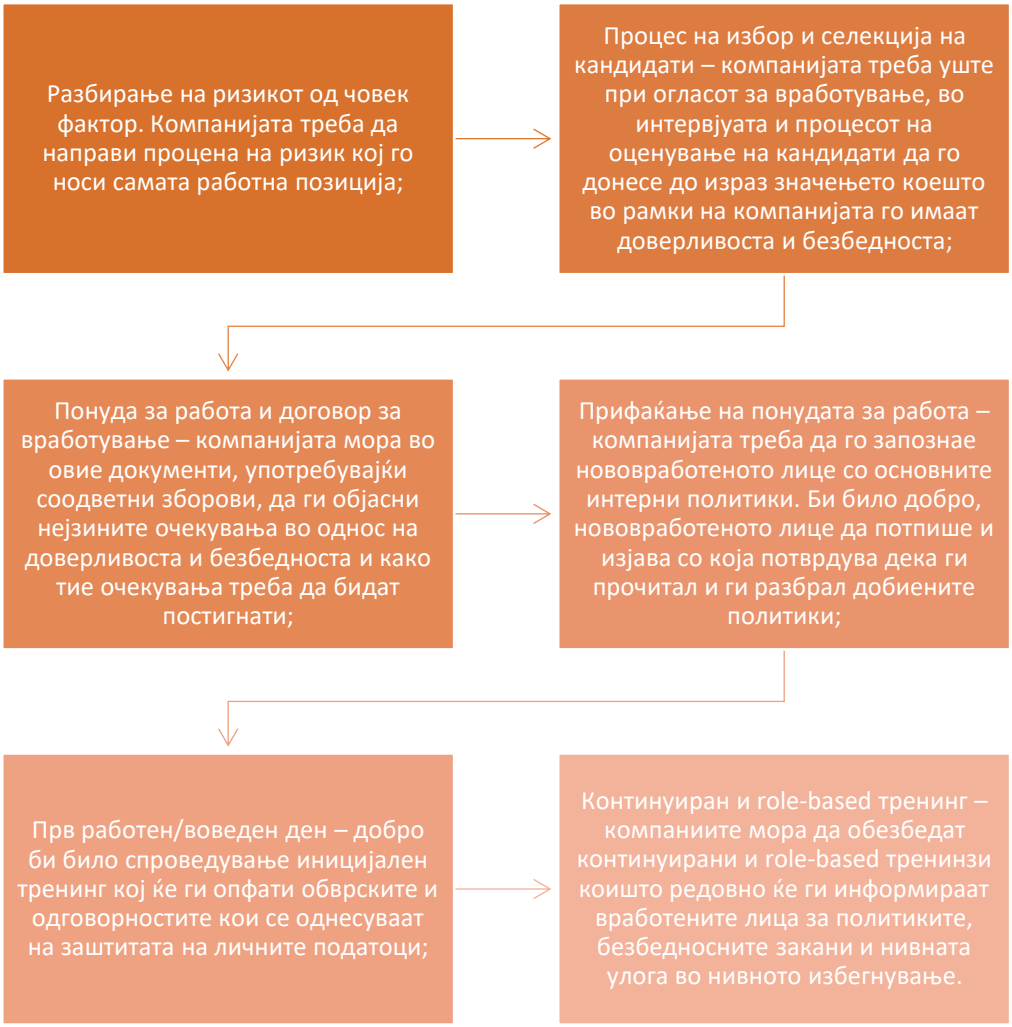
Со цел имплементирање на соодветни технички и организациски мерки, компаниите треба да имаат информиран и посветен менаџмент. Земајќи ги предвид искуствата и препораките на професионалците за информациска сигурност, се доаѓа до заклучок дека компаниите коишто немаат посветен менаџерски тим е поверојатно дека ќе страдаат од настани и ќе имаат зголемен ризик од настанување инциденти. Посветен менаџерски тим ќе придонесе за клучни придобивки за компанијата. На пример, безбедноста ќе биде третирана на ниво на менаџмент, менаџментот ќе се грижи за подигнување на свеста за ризици и заштита на личните податоци, ќе бидат доделени доволно ресурси и така натаму.

[39] „Службен весник на РСМ“ број 122 од 12.5.2020 година

[40] Член 7 од Правилникот за безбедност на обработката на личните податоци („Сл. весник на РСМ“ бр.122 од 12.5.2020 година)

Развивање култура во рамки на компанијата, и вработените лица како „внатрешна закана“

Препорака е менаџментот да ја моделира компанијата така што континуирано ќе развива култура за почитување на заштитата на личните податоци. Централен елемент на културата во една компанија е изборот на компетентни, доверливи и одговорни вработени лица. Клучни компоненти на овој процес би биле:



Политики, контроли и процеси – документација за безбедност

Не постои начин доволно да се нагласи важноста на соодветна документација за безбедност, имајќи предвид дека тоа е првиот чекор за постигнување на оперативна сигурност. Документацијата се воведува и со Законот за заштита на личните податоци кој во неколку наврати (data protection by design, проценка на влијанието на заштитата на личните податоци и принципот на транспарентност) ја нагласува обврската од креирање, дистрибуција и чување записи.

При креирање на документацијата, најраспространет е слоевитиот пристап. Според овој пристап, на најгорниот слој се документи од високо ниво со кои се дефинираат политиките на контролорот (политики). Во следниот слој се наоѓаат подетални документи со кои се

наведуваат контролите коишто ќе се имплементираат со цел да се постигнат политиките (процедури). Во третиот слој се наоѓаат најдеталните документи со кои се опишани оперативните процеси (упатства).

Технологијата при примена на принципот на безбедност

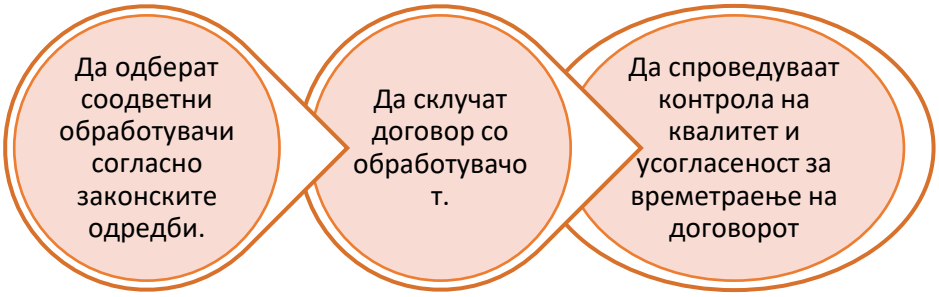
Може да заклучиме дека главниот акцент на регулативата за заштита на личните податоци е ставен на електронските информации. Оттука, компаниите мора да се осигураат дека нивната технологија може да ги задоволи барањата на принципот на безбедност. Освен енкрипцијата, постојат и други задолжителни барања, како што се антивирус, антиспам, firewall, управување со пристапи (access management), детекција на инциденти, превенција од губење податоци (data loss prevention), двофакторска автентификација и лог менаџмент. Секако, употребата на голем број од овие технологии, повлекува и прашања за приватноста на вработените лица (види глава 10 точка 1 од овој прирачник), поради што истите треба да се употребуваат на соодветен начин.

Физичка околина

Безбедна физичка околина е уште еден дел од генералната безбедност. Софистицирани контролни системи за влез, видеонадзор, заклучени плакари и политика на чисто биро се само дел од контролните мерки коишто им се на располагање на контролорите.

Управување со ризици од обработувачи и добавувачи

Контролорите мора:



Листа на предлог-чекори за проверка на обработувачот во пред договорниот период:

✓	Осигурување дека обработувачот е усогласен со законските одредби за заштита на личните податоци;
✓	Проверка дали обработувачот е или бил под истрага за нарушување на безбедноста на личните податоци;
✓	Проверка дали обработувачот е или бил под истрага за нарушување на безбедноста на личните податоци;
✓	Идентификација на другите клиенти на обработувачот;
✓	Проверка дали обработувачот е сертифициран според ISO27001, PCI DSS или некој друг стандард од областа на информацискатa сигурност;
✓	Ревидирање на документацијата на обработувачот за безбедност и заштита на личните податоци;
✓	Спроведување на on site посети и контроли;
✓	Идентификување на местото на седиштето на обработувачот;
✓	Запознавање со ланецот на набавка на обработувачот и неговите подизведувачи.

Членови 28–29, 32, 36-38 од Законот за заштита на личните податоци;
Членови 25, 28, 32-34 од Општата регулатива за заштита на личните податоци;
Правилник за безбедност на обработката на личните податоци, АЗЛП;
Правилник за начинот на известување за нарушување на безбедноста на личните податоци, АЗЛП

7. Отчетност (Accountability)

Одговорност на контролорот

Успешноста на контролорот да го примени принципот на отчетност се гледа низ призмата на усогласување со принципите на обработка на личните податоци[41] и способноста таа усогласеност да ја докаже. Воедно, контролорот мора да примени и соодветни технички и организациски мерки имплементирани врз основа на претходно спроведена процена на ризиците. Колку е поголем ризикот, толку построги треба да бидат мерките. Па се поставува прашањето, што мора да преземе контролорот со цел да постигне усогласеност со оваа

[41] Член 9 став (1) од Законот за заштита на личните податоци („Сл. весник на РСМ“ број 42 од 16.2.2020 година)

обврска? Има три клучни аспекти кои треба да се земат во разгледување: (1) интерни политики, (2) интерна алокација на одговорности и (3) тренинг.

Интерни политики

Темел на усогласеноста на контролорот е интерна политика за системот за заштита на личните податоци[42] со која ќе се исцртаат главните контури на системот за заштита на личните податоци и мерките што ќе се преземат при обработка на личните податоци. Политиката не треба само да ги пресликува законските принципи за обработка на личните податоци, туку да ги содржи најмалку следниве елементи:

Опсег	На кого се однесува политиката и кои видови на обработка на личните податоци ги опфаќа;
Изјава	Заложбите на компанијата во однос на заштитата на личните податоци и опис на целите за обработка на личните податоци;
Одговорност на вработените лица	Одговорност на вработените лица од аспект на обработката на личните податоци;
Одговорност на менаџментот	Одговорност на менаџментот од аспект на имплементирање и одржување на системот за заштита на личните податоци
Пријавување инциденти	Обврска за вработените лица да се пријавува секој инцидент;
Усогласеност на политиката	Правните последици од непочитување на правилата (граѓански и кривични постапки, како и дисциплинска постапка).

Интерна алокација на одговорности

Интерната алокација на одговорности ќе ја олесни супервизијата на Агенцијата, ќе им овозможи на субјектите на личните податоци да ги остварат своите права, и ќе овозможи навремено ажурирање на политиките, процедурите и процесите.

Контролорот може да состави тим за управување со заштитата на личните податоци кој би бил составен од претставници на секој сектор што е засегнат со обработка на личните податоци. Дополнително, контролорот може да назначи и лице кое ќе ја има примарната одговорност за системот за заштита на личните податоци (повеќе детали за назначувањето на офицер за заштита на личните податоци во точка 6 од оваа глава).

Тренинг

Контролорот треба да креира серија на тренинг програми дизајнирани со цел да ги информира вработените лица за правните обврски за заштитата на личните податоци. Од особено значење е овие тренинзи да не бидат генерални, односно да не биде еден тренинг за сите. Напротив, тренингот треба да биде креиран соодветно на работните обврски и одговорности за сите категории на вработени лица.

[42] Член 6, став (4) од Правилникот за безбедност на обработката на личните податоци („Сл. весник на РСМ“ бр. 122 од 12.5.2020), Агенција за заштита на личните податоци

Препорака е контролорот да го документира и мониторира спроведувањето на тренинг програмите, а со цел демонстрирање отчетност. Добра пракса е и испраќање редовни пораки до вработените лица кои би ги потсетувале на нивните обврски од аспект на заштитата на личните податоци, како и креирање централен сет на често поставувани прашања на компанискиот интранет, кои во одговорите би ги линкувале и соодветните политики или процедури.

Заштита на личните податоци by design и by default[43]

Заштита на личните податоци by design

Според принципот на заштита на личните податоци by design соодветни технички и организациски мерки треба да се вградат во процесот на обработка на личните податоци уште во моментот на дефинирање на средствата на обработка. Погрешно би било сфаќањето дека овој принцип се применува само во фазите на планирање и реализација на нови средства за обработка. Напротив, овој принцип треба да се применува и при тековни активности и средства за обработка, за да се осигура контролорот дека ефективно се справува со целиот животен век на личните податоци коишто ги обработува.

Заштита на личните податоци by default

Контролорот има обврска да имплементира соодветни технички и организациски мерки со кои ќе се осигура дека по default ги обработува само оние лични податоци коишто се неопходни за постигнување на целта на конкретната обработка. Тоа значи дека со имплементираните мерки контролорот, по default, ќе го обработува само неопходното количество на лични податоци, во опсег кој е неопходен за исполнување на целта на конкретната обработка, и со време на чување и достапност сè до исполнување на конкретната цел на обработка.

Како да се усогласат компаниите (контролорите и обработувачите)

Со цел да постигнат усогласеност, компаниите треба внимателно да ги ревидираат и проценат системите и процесите за обработка на личните податоци и, меѓу другото, да одредат:

- Дали личните податоци се соодветно мапирани, класифицирани, означени, чувани и достапни, а со цел да бидат лесно најдени и издвоени во случај на одредено барање на субјектот на личните податоци (на пр. бришење, примена, примерок...);
- Дали системите се подесени за автоматско бришење на лични податоци (на пр. дали системот има имплементирано технички мерки со кои по истекот на рокот на чување на личните податоци, ги обележува оние кои треба да бидат избришани);
- Дали хартиените формулари се составени на начин што нема да бараат поголема количина на лични податоци од онаа којашто е неопходна;
- Дали личните податоци може да бидат псевдонимизирани;
- Дали личните податоци може да се издвојат за да им се исполни правото на субјектите на личните податоци кои приговориле на пораките за директен маркетинг; и

[43] Член 29 од Законот за заштита на личните податоци („Сл. весник на РСМ“ број 42 од 16.2.2020 година)

- Дали личните податоци се структурирани во вообичаено користен и машински читлив формат за да им овозможи на компаниите да може да исполнат барања за преносливост на личните податоци.

Документација и соработка со Агенцијата за заштита на личните податоци

Со новата законска регулатива се укинува обврската на контролорите пред започнување со која било обработка на личните податоци да ја известуваат Агенцијата за заштита на личните податоци. Наместо тоа, контролорите ќе мора да чуваат документација и евиденција за нивната обработка на лични податоци, во хартиена или електронска форма, и да ги направат достапни на барање на Агенцијата за заштита на личните податоци.[44] Исклучок постои во ситуациите кога контролорот врши обработка на лични податоци со висок ризик за правата и слободите на физичките лица, за што мора да биде известена Агенцијата за заштита на личните податоци.

Кои документи и записи мора да ги чува компанијата

Според законот, контролорите и обработувачите треба да водат евиденција на активностите за обработката на личните податоци. Од оваа обврска се ослободени контролорите и обработувачите коишто имаат помалку од 50 вработени, освен (1) ако постои веројатност обработката којашто ја вршат да претставува ризик за правата и слободите на субјектите на личните податоци, (2) ако обработката е честа, односно не е повремена, или (3) ако се обработува посебна категорија на лични податоци и лични податоци за казнени осуди и казнени дела.

Освен документацијата којашто е задолжителна според законот, за да може да ги докаже и оправда своите одлуки, препорака е контролорот да води и други записи за донесените одлуки кои се однесуваат на обработката на личните податоци.

Пример: Компанијата Х планира да ги обработува личните податоци коишто веќе ги има, но за исполнување на нова цел. По спроведената проценка компанијата Х утврдила дека новата цел за обработка е во согласност со првичната цел за којашто биле собрани личните податоци, но утврдила и дека не постои конкретна законска обврска да ја документира оваа проценка. Сепак, водејќи се од принципот за отеченост, компанијата Х прави запис од спроведената проценка, во којшто воедно ја оправдува донесената одлука, сè со цел да може да ја демонстрира својата усогласеност со одредбите од законот.

[44] Член 34 од Законот за заштита на личните податоци („Сл. весник на РСМ“ број 42 од 16.2.2020 година)

Известување за обработка на лични податоци со висок ризик

Кога при користење технологии за некој вид на обработка, земајќи ги предвид природата, обемот, контекстот и целите на обработката на лични податоци, постои веројатност истата да предизвика висок ризик за правата и слободите на физичките лица, а во функција на отчетноста, контролорот ја известува Агенцијата.[45] Во суштина, начинот и системот на известување е прилично сличен на претходниот начин и систем за регистрирање и пријавување збирки на лични податоци во централниот регистар на, тогаш, ДЗЛП, со таа разлика што сега се евидентираат само збирките на лични податоци со висок ризик[46].

Проценка на влијанието на заштитата на личните податоци (DPIA)[47]

Проценката на влијанието на заштитата на личните податоци (Data protection impact assessments – DPIA) како алатка може да се користи од страна на контролорите со цел да ги идентификуваат и адресираат сите проблеми со обработката на личните податоци коишто може да настанат при развој на нови продукти или услуги, или при преземање нови активности кои вклучуваат обработка на лични податоци. Освен на добра волја, проценката на влијанието на заштитата на личните податоци е и законска обврска на контролорите пред започнување на обработка на лични податоци со користење на нови технологии, и обработка која може да има висок ризик за правата и слободите на физичките лица.

Агенцијата за заштита на личните податоци објави и Листа на видови на операции на обработка за кои се бара проценка на влијанието врз заштитата на личните податоци[48], но истата не е ограничувачка од причина што секогаш треба да се зема предвид и веројатноста дека некоја обработка која не се наоѓа на Листата може да предизвика висок ризик за правата и слободите на физичките лица.

Фази на спроведување на DPIA

Проценката на влијанието на заштитата на личните податоци се спроведува во четири фази[49] според претходно донесена Методологија за спроведување проценка на влијанието на заштитата на личните податоци.[50]

[45] Член 71 од Законот за заштита на личните податоци („Сл. весник на РСМ“ број 42 од 16.2.2020 година)
[46] „Службен весник на РСМ“ број 122 од 12.5.2020 година
[47] Член 39 од Законот за заштита на личните податоци („Сл. весник на РСМ“ број 42 од 16.2.2020 година)
[48] „Службен весник на РСМ“ број 122 од 12.5.2020 година
[49] Член 11 од Правилникот за процесот на проценка на влијанието на заштитата на личните податоци („Сл. весник бр. 122 од 12.5.2020 година)
[50] Член 10 од Правилникот за процесот на проценка на влијанието на заштитата на личните податоци („Сл. весник бр. 122 од 12.5.2020 година)

Што доколку обработката е со висок ризик и по спроведената DPIA?

Доколку по спроведување на проценката на влијанието на заштитата на личните податоци се покаже дека обработката е со висок ризик, и дека нема соодветни мерки кои може да го намалат ризикот, контролорот мора да се консултира со Агенцијата за заштита на личните податоци. Она што контролорите особено треба да го предвидат е дека оваа законска обврска претходи на отпочнувањето со обработката, па така комуникацијата со Агенцијата, која има законски рок од 60 дена да даде консултација, може временски да ги одложи планираните нови процеси за коишто е потребна предметната обработка.

Офицер за заштита на личните податоци

Позицијата офицер за заштита на личните податоци не е новина во македонското законодавство. Воведена е со измените на Законот за заштита на личните податоци во 2010 година,[51] и како законска обврска се наметна на сите компании со повеќе од 10 вработени. Со новиот закон, офицерот за заштита на личните податоци се наметнува како обврска независно од бројот на вработени, туку во зависност од видот на обработката којашто контролорот, односно обработувачот ја спроведува.

[51] „Сл. весник на РМ“ број 124/10 година

Кој може да биде офицер за заштита на лични податоци?

Вработено лице

Надворешно ангажирано лице

- активно да го користи македонскиот јазик,
- со правосилна судска пресуда да не му е изречена казна или прекршочна санкција забрана за вршење на професија, дејност или должност,
- да има завршено високо образование, и
- да има стекнати знаења и вештини по однос на практиките и прописите за заштита на личните податоци,
- ако извршува други работни задачи, тие задачи да не доведуваат до судир на интерес.

Улога на офицерот за заштита на личните податоци[52]

Компанијата мора да обезбеди вклученост на офицерот за заштита на личните податоци во сите прашања поврзани со заштитата на личните податоци.[53] Исто така, компанијата мора да му гарантира на офицерот и поддршка на начин што ќе му ги даде на располагање сите потребни ресурси кои се неопходни за исполнување на работите од негова надлежност, но и на начин што ќе вложува во унапредување на неговото знаење и експертиза.

Други мерки за отчетност – задолжителни корпоративни правила

Друга мерка која може да придонесе за отчетност на компанијата се задолжителните корпоративни правила[54] т.н. „златен стандард“ на системите за заштита на личните податоци. Иницијално, целта на овие правила е да се овозможи прекугранично пренос на лични податоци во рамки на една меѓународно распространета корпоративна групација, на начин што сите членови на групацијата ќе обезбедат исто ниво на заштита на личните податоци со примена на сет од задолжителни правила. Овие правила се сметаат за „златен стандард“ бидејќи компаниите пред нивната имплементација мора да ја оправдаат нивната законска усогласеност пред надлежната Агенција за заштита на личните податоци. Доколку Агенцијата ја одобри примената на овие правила, тие на некој начин ќе претставуваат алатка за демонстрирање на отчетноста на компанијата.

Членови 29, 34, 39-43, 45, 51, 71 од Законот за заштита на личните податоци;
Членови 25, 30, 35-39 од Општата регулатива за заштита на личните податоци;
Правилник за безбедност на обработката на личните податоци;
Правилник за известување за обработка на лични податоци со висок ризик;
Правилник за процесот на проценка на влијанието на заштитата на личните податоци;
Guidelines on Data protection Officers (DPO), WP29;
Guidelines on DPIA and determine whether processing is likely to result in high risk for the purposes of GDPR, WP29.

[52] Член 43 од Законот за заштита на личните податоци (Сл. Весник на РСМ број 42 од 16.02.2020 година)
[53] Член 42 од Законот за заштита на личните податоци (Сл. Весник на РСМ број 42 од 16.02.2020 година)
[54] Член 51 од Законот за заштита на личните податоци („Сл. весник на РСМ“ број 42 од 16.2.2020 година)

8. Пренос на податоци

Секој пренос на лични податоци за кои постои намера да бидат обработувани во земјата каде што ќе се пренесат, може да се спроведе само доколку се исполнети одредени законски услови. За преносот на личните податоци да потпадне под капата на законската регулатива треба да бидат исполнети два услови. Првиот услов е постоењето на намера пренесените лични податоци да се обработуваат во трета земја, и тука не потпаѓа едноставниот транзит на личните податоци низ територијата на некоја земја. Вториот услов е земјата каде што се пренесуваат личните податоци да не е членка на Европската Унија, односно во европскиот економски простор. За пренос во земјите членки на Европската Унија, односно во европскиот економски простор, контролорот односно обработувачот има обврска само да ја извести Агенцијата за заштита на личните податоци[55] во рок од 15 дена пред започнување на преносот на личните податоци.[56]

Контролорот или обработувачот може да извршат пренос на лични податоци во земји надвор од ЕУ, односно ЕЕП, само во ситуации кога е загарантирано нивото на заштита на физичките лица. Во прилог е даден краток опис на ситуациите во коишто може да се изврши ваков пренос.

Контролор од Франција пренесува лични податоци на контролор во Германија (двете држави се во ЕЕП) преку сервер којшто се наоѓа во Австралија. Не постои намера личните податоци да се обработуваат во Австралија, туку таквата обработка ќе се врши во Германија. Па така, се смета дека преносот на лични податоци се врши само во Германија.

Пренос на лични податоци врз основа на одлука за соодветност[57]

Во надлежност на Агенцијата за заштита на личните податоци е носењето на одлуки за соодветност на степенот на заштита на личните податоци во трета држава каде што е планиран преносот на личните податоци. Со други зборови, пренос на лични податоци ќе може да се врши во држави за коишто Агенцијата ќе одлучи дека обезбедуваат соодветно ниво на заштита на личните податоци. Ваква одлука Агенцијата ќе ја донесе по претходно барање од страна на контролорот или обработувачот поднесено најдоцна 15 дена пред започнување на преносот на личните податоци.[58]

[55] Член 48, став (3) од Законот за заштита на личните податоци („Сл. весник на РСМ“ број 42 од 16.2.2020 година)

[56] Член 2, став (2) од Правилникот за пренос на лични податоци („Сл. весник на РСМ“ број 122 од 12.5.2020 година) донесен од Агенцијата за заштита на личните податоци

[57] Член 49 од Законот за заштита на личните податоци („Сл. весник на РСМ“ број 42 од 16.2.2020 година)

[58] Член 3 од Правилникот за пренос на лични податоци („Сл. весник на РСМ“ број 122 од 12.5.2020 година) донесен од Агенцијата за заштита на личните податоци

Пренос на лични податоци кој подлежи на соодветни заштитни мерки[59]

Контролорот или обработувачот може да извршат пренос на лични податоци и во држави за кои Агенцијата за заштита на личните податоци нема донесено одлука за соодветност, но само под услов да обезбедат соодветни заштитни мерки, и субјектите на личните податоци да имаат можност на судска заштита. Законот наложува соодветните заштитни мерки да бидат предвидени преку:

- правно обврзувачки и извршни инструменти меѓу јавните органи или тела (билатерални договори);
- задолжителни корпоративни правила;
- стандардни клаузули за заштита на личните податоци кои ги утврдува Агенцијата или кои се одобрени од страна на Европската комисија;
- одобрен кодекс на однесување[60] со обврзувачки и извршни обврски на контролорот или обработувачот во третата земја за применување соодветни заштитни мерки, вклучувајќи и одредби во однос на правата на субјектите на лични податоци; или
- одобрен механизам за сертификација[61] заедно со обврзувачки и извршни обврски на контролорот или обработувачот во третата земја за применување на соодветни заштитни мерки, вклучувајќи и во однос на правата на субјектите на лични податоци.

Агенцијата ќе го дозволи ваквиот пренос на лични податоци на претходно барање од страна на контролорот или обработувачот, кое меѓу другото мора да содржи и опис на предвидените соодветни заштитни мерки.[62]

Пренос на лични податоци во рамки на меѓународна корпорациска групација

Една од поголемите новини во регулативата во однос на меѓународниот пренос на лични податоци е вклучувањето на Задолжителните корпоративни правила (Binding corporate rules – BCR)[63] како механизам достапен на контролорите и обработувачите за да го легализираат преносот на личните податоци внатре во рамки на нивната корпоративна групација. Овие правила, кои претходно треба да бидат одобрени од Агенцијата, мора да се правно обврзувачки за секој засегнат член на групацијата.

[59] Член 50 од Законот за заштита на личните податоци („Сл. весник на РСМ“ број 42 од 16.2.2020 година)
[60] Член 44 од Законот за заштита на личните податоци („Сл. весник на РСМ“ број 42 од 16.2.2020 година)
[61] Член 46 од Законот за заштита на личните податоци („Сл. весник на РСМ“ број 42 од 16.2.2020 година)
[62] Член 4 од Правилникот за пренос на лични податоци („Сл. весник на РСМ“ број 122 од 12.5.2020 година) донесен од Агенцијата за заштита на личните податоци
[63] Член 51 од Законот за заштита на личните податоци („Сл. весник на РСМ“ број 42 од 16.2.2020 година)

Пренос на лични податоци во специфични ситуации[64]

Во отсуство на одлука за соодветност или на соодветни заштитни мерки, преносот на личните податоци сепак ќе може да се изврши доколку е исполнет некој од следните услови:

- постои изречна согласност на субјектот на личните податоци, откако претходно бил информиран за сите ризици од таквиот пренос;
- поради извршување договор помеѓу контролорот и субјектот на личните податоци како договорни страни, или за спроведување преддоговорни активности;
- поради склучување или извршување на договор помеѓу контролорот и трето лице, а во интерес на субјектот на личните податоци;
- доколку преносот е неопходен поради важни причини од јавен интерес;
- доколку преносот е неопходен за спроведување правни барања;
- доколку преносот е неопходен за заштита на суштинските интереси на субјектот на личните податоци, а субјектот е деловно неспособен за да даде согласност; и
- доколку преносот се врши од регистар кој според закон има за цел да обезбеди информации за јавноста и кој е отворен за консултации со јавноста или на кое било лице кое може да докаже легитимен интерес.

И доколку не е исполнет ниту еден од наведените услови, преносот на личните податоци сепак би можел да се изврши, но само доколку не е повторувачки карактер и се однесува на ограничен број на субјекти на лични податоци, а истиот е потребен за исполнување на легитимните интереси на контролорот над кои не преовладуваат интересите или правата и слободите на субјектот на лични податоци, при што контролорот ги оценил сите околности поврзани со преносот на личните податоци и врз основа на таа проценка обезбедил соодветни заштитни мерки во однос на заштитата на личните податоци. За овој пренос, контролорот мора да ја информира Агенцијата за заштита на личните податоци.

Членови 48-56 од Законот за заштита на личните податоци;
Членови 44-50 од Општата регулатива за заштита на личните податоци;
Правилник за пренос на личните податоци;

9. Обработка на лични податоци во работни односи

Во работниот однос, работодавачот обработува лични податоци на вработените за исполнување на различни цели. Во тој однос, работодавачот ја има улогата на контролор со сите свои обврски и одговорности, додека пак вработените ја имаат улогата на субјекти на лични податоци со сите нивни права.

[64] Член 53 од Законот за заштита на личните податоци („Сл. весник на РСМ“ број 42 од 16.2.2020 година)

Законски основ за обработка на личните податоци на вработените

Исполнување на договорот за вработување

Контролорот како работодавач, голем дел од процесите на обработката на личните податоци на вработениот може да ги заснова на исполнување на правата и обврските од договорот за вработување. Пример за таква обработка би била обработката на името и презимето и бројот на трансакциската сметка на вработениот за исплата на плата.

Исполнување на законски обврски на контролорот

Одредени закони може да му наметнат на контролорот одредени обврски чие исполнување би подразбирало обработка на личните податоци на вработените. Таков е примерот со давање информации на даночните органи за платите кои контролорот им ги исплаќа на вработените лица.

Легитимен интерес на контролорот

Постојат многу ситуации во кои контролорот може да ја заснова обработката на лични податоци на вработените лица на сопствениот легитимен интерес. Таков е примерот со пренесување на личните податоци на вработените од стара на нова апликација за пресметка на плати.

Согласност

Согласноста како законски основ за обработка на личните податоци претставува лизгав терен кога станува збор за нејзината валидност во работните односи. За согласноста да биде валидна потребно е да биде дадена доброволно, за што како услов се наметнува постоењето на баланс помеѓу позициите на контролорот и субјектот на личните податоци. Дали таков баланс постои помеѓу позициите на работодавачот како контролор и субјектот на личните податоци како вработено лице? Според Мислењето на Европското тело за заштита на личните податоци „постои дисбаланс на позициите во контекст на работните односи“.[65] Ова се јавува како резултат на претпоставката дека вработените може да чувствуваат притисок да се согласат за одредена обработка на нивните лични податоци поради моќта на позицијата којашто ја има контролорот како работодавач, и поради притисокот дека извршувањето на договорот за вработување е условено со давањето на согласноста. Но како и да е, тоа не значи дека работодавачите во ниту еден случај не можат да ја засноваат обработката на личните податоци на вработените на нивна согласност. Земајќи ја предвид нееднаквоста во позициите на моќ, вработените сепак можат да дадат доброволна согласност во исклучителни ситуации кога прифаќањето или одбивањето на давање на согласноста нема да произведе никакви последици по договорот за вработување.[66] Но, останува обврска на работодавачот како контролорот да докаже дека согласноста е дадена доброволно и дека истата е валидна.

[65] Page 7 from Guidance on consent under Regulation 2016/679, adopted 28.11.2017
[66] Page 23, paragraph 6.2 from Opinion 2/2017 on data processing at work (WP29), adopted 8.6.2017

Посебни категории на лични податоци на вработените лица

При обработка на посебните категории на лични податоци на вработените лица, контролорот како работодавач мора да се осигура дека постои некој од исклучоците предвидени во членот 13 од Законот за заштита на личните податоци кога е дозволена обработката на овие лични податоци.

Известување на вработените за обработка на нивните лични податоци

Независно од законскиот основ за обработка на личните податоци на вработените лица како субјекти на лични податоци, обврска на работодавачот како контролор е да ги информира[67] за обработката на нивните лични податоци, за целите на обработката, кои им се правата и кому да се обратат за нивно остварување. Работодавачот како контролор може да одлучи начинот на информирање да биде преку Прирачник за вработени или преку конкретен допис, достапен до сите вработени, како што на пример е интранетот.

Чување досие на вработени

Работодавачот како контролор започнува да обработува лични податоци на вработениот како субјект на лични податоци уште од моментот кога субјектот на личните податоци аплицира за работната позиција. Од записи за процесот на избор на кандидати за вработување, боледувања, едукација, плата, евалуации на перформанс, контролорот обработува голема количина на лични податоци за вработените. За голем број од тие податоци постојат законски дефинирани рокови на чување коишто контролорот мора да ги почитува, но за останатите контролорот мора сам со свои интерни акти да дефинира разумен рок водејќи се од максимата дека ниту еден податок не живее вечно. Освен рокот на чување, контролорот мора да го осигура и пристапот до овие лични податоци. На пример, по прекин на работниот однос контролорот треба дополнително да го лимитира пристапот до досието на заминатиот вработен, од причина што секторот за човечки ресурси повеќе нема потреба на дневна основа да пристапува до овие податоци.

Мониторирање на работното место и заштита од губење податоци

Вработените лица не го губат правото на приватност кога се на своите работни места, но нивната приватност е балансирана со легитимните права на работодавачот да го спроведува деловното работење и да ја штити компанијата од какви било несоодветни активности на вработените.

Позадинска проверка на потенцијалните и постоечките вработени

Многу честа активност на секторот за човечки ресурси е позадинска проверка на потенцијалните и постоечките вработени. Позадинската проверка се врши на повеќе нивоа, од проверка на лицето на социјалните медиуми, верификација на образовните квалификации, па сè до проверка на минати криминални активности. Една од главните причини за позадинската проверка е фактот што факторот човек е најслабата алка во една организација од аспект на безбедноста на податоците.

[67] Член 17 и 18 од Законот за заштита на личните податоци („Сл. весник на РСМ“ број 42 од 16.2.2020 година)

Превенција од губење на податоци (Data Loss Prevention - DLP)

Технологиите за превенција од губење податоци во последните неколку години добија на голема популарност. Компаниите ги користат како алатки за да ги заштитат својата ИТ-инфраструктура и доверливите бизнис-информации од надворешни и внатрешни закани. Овие алатки вклучуваат обработка и на личните податоци на вработените кои работат на системите и мрежите на работодавачот. Затоа се смета дека „употребата на овие DLP-алатки е форма на мониторирање на вработените, иако главната намера за употреба е превенција од загуба на компаниски податоци".[68]

Мониторирање на вработените

Работодавачот може да донесе одлука да ги мониторира вработените, која одлука може да ја заснова на повеќе причини, како што се на пример начинот на употреба на опремата за работа или сомнително неавторизирано однесување. Но доколку работодавачот донесе ваква одлука, прво мора да се осигура дека е усогласен со наведените принципи за обработка на личните податоци:

- *Неопходност* – работодавачот мора да може да демонстрира дека мониторирањето навистина е неопходно;
- *Законитост* – работодавачот мора да има законски основ за обработка на личните податоци;
- *Пропорционалност* – секое мониторирање мора да биде пропорционално на проблемот со кој што се соочува работодавачот; и
- *Транспарентност* – работодавачот мора јасно да го информира вработениот дека ќе се спроведува мониторирање.

Bring your own device

Многу работодавачи дозволуваат вработените да ги користат своите приватни уреди (на пр. паметни телефони, таблети) за работни потреби. На пример, вработениот може да го постави службениот e-mail на приватниот уред, така што од еден уред ќе пристапува и до приватните и до службените е-мејлови. Во вакви ситуации се јавуваат одредени предизвици за усогласеност со правилата за заштита на личните податоци, бидејќи работодавачот како контролор е одговорен за сите лични податоци кои се обработуваат на уредот на вработениот за цели поврзани со работата. Истовремено, уредот содржи и лични податоци на вработениот до коишто работодавачот нема законска причина да пристапува. Но фактот дека уредот содржи деловни податоци му дава на работодавачот право да бара од вработениот силна заштита на уредот. Препорака е компаниите кои применуваат користење на приватни уреди да:

- воведат политика за користење приватни уреди за деловни потреби со која ќе се дефинира начинот на користење на уредите, како и одговорностите на вработените;
- бидат јасни околу тоа каде ќе се чуваат податоците обработувани преку уредот и кои мерки мора да бидат преземени за податоците да бидат безбедни;
- осигураат дека преносот на податоци од уредот до компаниските сервери ќе биде безбеден;
- најдат начин како да се справат со личните податоци зачувани на уредот во случај губење на уредот или доколку вработениот ја напушти компанијата. На пример може

[68] Point 14.6.2 from European Data Protection Law and Practice, IAPP, 2018

да се користи софтвер за управување со мобилни уреди со кои може да се лоцира уредот и да се избришат податоците коишто се наоѓаат на него.

Член 85 од Законот за заштита на личните податоци;
Член 88 од Општата регулатива за заштита на личните податоци;

10. Активности за надзор и мониторинг

Надзорот станува сè полесен. Опремата што се користи за мониторирање и надзор станува сè поевтина и пософистицирана, софтверите овозможуваат покомплексна аналитика на податоци, а технологијата што се користи продуцира сè повеќе и повеќе податоци за физичките лица. Целта на одредбите за приватност и заштита на личните податоци, во оваа смисла, е да го регулира, ограничи и да го услови надзорот за да се осигура дека кога веќе се врши надзор кој de facto е инвазија врз приватноста, таа инвазија е неопходна, законска, фер и пропорционална.

Комуникациски податоци

Во оваа точка од Прирачникот ќе бидат земени предвид комуникациските податоци коишто се резултат на електронската комуникација, како комуникација која е најчеста во деловните процеси на компаниите.

Видеонадзор

Законитост на обработката

Многу малку е веројатно контролорот да се потпре на согласноста како законски основ за обработка на личните податоци добиени преку видеонадзор, од причина што видеонадзорот опфаќа голем број на субјекти на лични податоци. Најлогичната законска основа во овој случај би била легитимниот интерес којшто го има контролорот, за што треба да претходи спроведен тест за избалансираност помеѓу легитимниот интерес на контролорот наспроти правата и слободите на физичките лица.

Проценка на влијанието на заштитата на личните податоци

Доколку видеонадзорот претставува висок ризик, или пак вклучува систематско набљудување на јавен простор во голем размер, контролорот мора да спроведе проценка за влијанието на заштитата на личните податоци. Како мерки коишто контролорот може да ги имплементира за да ги заштити личните податоци на субјектите, се препорачуваат:

- *Обука на вработените* – Вработените коишто работат со системите и кои имаат пристап до видеонадзорот треба да имаат конкретна обука и да се запознаат со нивните обврски и одговорности;
- *Правилник за начинот на вршење на видеонадзор;*[69]
- *Периодична оценка* – анализа на целта/целите за која се поставува видеонадзорот и периодични оценки на постигнатите резултати од системот за видеонадзор.

Видеонадзор и права на субјектите на личните податоци

Контролорот мора да го почитува принципот на транспарентност до степен којшто е возможен во случаи кога нема директен однос со субјектите на личните податоци (на пр, случајни минувачи). Тоа ќе го оствари со јавно известување[70] кое ќе информира дека се врши видеонадзор, кој го врши, и на кој начин може да се добијат дополнителни информации. Исто така, за остварување на правата на субјектите, контролорот треба да донесе и Изјава за приватност[71] како составен дел од Правилникот за начинот на вршење на видеонадзор.

Редовна контрола на системот за видеонадзор

Контролорот пред започнување на процесот на видеонадзор треба да направи анализа на целите за коишто се поставува видеонадзорот, а потоа на секои две години да прави периодична оценка на постигнатите резултати од овој систем. И во двата видови на контроли, нагласен е принципот на неопходност, односно дали самиот видеонадзор, или видеонадзорот во таков обем е навистина неопходен за постигнување на целите на контролорот.

[69] Правилникот за содржината и формата на актот за начинот на вршење на видеонадзор („Сл. весник на РСМ“ број 122 од 12.5.2020 година) донесен од Агенцијата за заштита на личните податоци

[70] Образец бр. 3 од Правилникот за содржината и формата на актот за начинот на вршење видеонадзор („Сл. весник на РСМ“ број 122 од 12.5.2020 година) донесен од Агенцијата за заштита на личните податоци

[71] Образец бр. 4 од Правилникот за содржината и формата на актот за начинот на вршење видеонадзор („Сл. весник на РСМ“ број 122 од 12.5.2020 година) донесен од Агенцијата за заштита на личните податоци

Агенцијата за заштита на личните податоци има пропишани обрасци[72] за спроведување на анализата и на периодичната оценка, што на контролорите ќе им помогне од аспект на дефинирање и спроведување на процесот на контрола.

Биометриски податоци

Биометриски се оние 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 овозможува или потврдува единствената идентификација на физичкото лице. Пример за биометриски податоци се: ДНК, отпечаток од прст, рожница, ирис, глас, лице, ракопис, одење итн. Биометриските системи денес се користат, најчесто, за две главни цели: (1) идентификација – кој си ти?, (2) автентификација – дали ти си тој што тврдиш дека си? За биометриските податоци да се сметаат за посебна категорија на лични податоци треба целта за нивната обработка да биде единствена идентификација на физичко лице. Доколку биометриските податоци се користат за друга цел, тогаш нема да се сметаат за посебна категорија на лични податоци, но секако ќе важат правилата за лични податоци.

Податоци за локација

Услугите коишто се базирани на локација користат информации за локацијата каде што треба да се испорача услугата. Тоа се апликации и сервиси од типот на социјални мрежи и игри, забава, реклама и маркетинг, навигација, плаќање, следење на добра и луѓе, безбедност и слично. Вообичаено, услугите коишто се базирани на локација се потпираат на техничката можност да го лоцираат подвижниот уред, како што е мобилен телефон, GPS receiver-от, чипот на платежната картичка и така натаму. Доколку податокот за локација сам или во комбинација со друга информација може да идентификува конкретно физичко лице, тогаш треба да се смета за личен податок. Имајќи го предвид трендот на развивање на бизнис-модели кои ги користат податоците за локација како главни влезни параметри, контролорот треба да процени кога употребата на мобилната апликација која користи податоци за локација може да резултира со висок ризик за корисникот на апликацијата, па во тој случај да го процени влијанието на заштитата на личните податоци.

Членови 89-93 од Законот за заштита на личните податоци;
Правилник за содржината и формата на актот за начинот на вршење на видео надзор;
Правилник за содржината на анализата на целта, односно целите за која се поставува видеонадзорот и извештајот од извршената периодична оценка на постигнатите резултати од системот за видеонадзор;
Guidelines on processing of personal data through video devices, WP29.

[72] Образец 1 и 2 од Правилникот за содржината на анализата на целта, односно целите за која се поставува видеонадзорот и извештајот од извршената периодична оценка на постигнатите резултати од системот за вршење видеонадзор („Сл. весник на РСМ“ број 122 од 12.5.2020 година) донесен од Агенцијата за заштита на личните податоци

11. Директен маркетинг

Концептот на директен маркетинг ја опфаќа секоја комуникација, остварена преку кои било средства за презентирање маркетинг-материјал или рекламирање, која е насочена кон одредено физичко лице. Тоа значи дека правилата за заштита на личните податоци ќе се применуваат при праќањето на маркетинг-пораки, само доколку се обработуваат лични податоци за да се искомуницира со субјектите на тие лични податоци. Пример на маркетинг-пораки кои не се сметаат за директен маркетинг се:

- *Маркетинг-комуникација која не е насочена кон физички лица* (на пр. банер на веб-страница , e-mail пораки пратени до компании без притоа да се спомнуваат контакти на физички лица) и
- *Пораки кои по својата природа се сервисни* (на пр. пораки испратени до физички лица кои се однесуваат на статус на испорака на нарачка).

Маркетингот vis-à-vis Законот за заштита на личните податоци

Секогаш кога се обработуваат лични податоци за целите на директниот маркетинг, контролорот мора да постапува според сите правила кои ги поставува Законот за заштита на личните податоци. Тоа се:

- Да се осигура дека постои законски основ за обработка (принцип на законитост). Согласно природата на обработката, тоа би бил легитимниот интерес или валидна согласност на субјектот на личните податоци;
- Да го информира субјектот на личните податоци за обработката на личните податоци за целите на маркетингот (принцип на транспарентност);
- Да имплементира соодветни технички и организациски мерки за заштита на личните податоци, вклучувајќи и писмен договор со задолжителни одредби склучен со обработувачот кој ќе врши директен маркетинг во име на контролорот (на пр. маркетинг-агенции);
- Да не врши пренос надвор од европскиот економски простор, освен доколку не се исполнети законските услови кои дозволуваат овој пренос да се изврши. На пример, листата со контакти не треба да се праќа во маркетинг-агенции од трети земји без контролорот да се осигура дека не се исполнети соодветните законски услови; и
- Да ги исполни сите други барања на Законот за заштита на личните податоци.

Право на opt-out

Правото на opt out се применува кога обработката на личните податоци за цели на директен маркетинг е засновано на согласност или на легитимниот интерес на контролорот. Според законот:

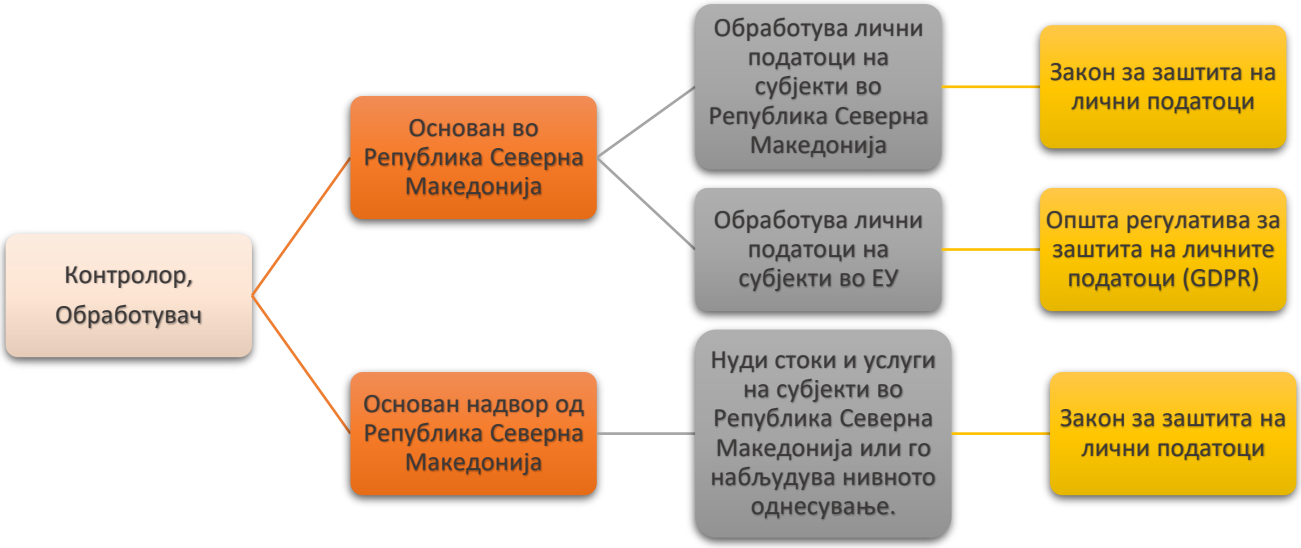
- Субјектите на личните податоци мора да се информирани за своето право на opt out;
- Лицата одговорни за маркетинг мора на субјектите на личните податоци да им го овозможат правото да направат opt-out преку сите канали на комуникација;
- Контролорот ќе го реализира барањето за opt-out навремено и без никакви трошоци; и
- По реализирање на правото на opt out, контролорот мора да ја прекине обработката и на податоците добиени од профилирањето.

При остварување на правото на opt out од страна на одреден субјект на личните податоци, контролорите наместо да ги избришат контакт-податоците, препорака е да ги „исклучат“ од употреба. Со бришење на податоците, контролорите ризикуваат после некое време повторно да ги маркетираат субјектите кои го остариле правото на opt-out. Но доколку ги „исклучат“ од употреба податоците, контролорот ќе има запис дека на тој субјект на личните податоци не треба да му се врши директен маркетинг бидејќи побарал opt out.

Член 96 од Законот за заштита на личните податоци;
Рецитал 70 од Општата регулатива за заштита на личните податоци;
Guidelines on processing of personal data through video devices, WP29.

12. Интернет-технологија и комуникации

Важечко право



Во натамошниот текст од ова поглавје нема да се нагласува разликата помеѓу европската и националната регулатива, од причина што и двете регулативи се идентични во однос на обврските и одговорностите кои ги опфаќа оваа тема.

Cloud

Услугите на cloud технологијата може да вклучуваат софтвер, инфраструктура (сервери), хостинг и платформи (оперативни системи). Примената на оваа технологија е широка, од личен веб e-mail, па сè до чување корпоративни податоци, и може да се подели во три модели: (1) IaaS – обезбедување инфраструктура, (2) PaaS – обезбедување платформа и (3) SaaS – обезбедување софтвер.

Cloud провајдер - контролор или обработувач

Како што беше споменато претходно во овој прирачник, главниот критериум за разлика помеѓу контролорот и обработувачот е во тоа кој одредува зошто и како се обработуваат податоците, а кој ги обработува податоците според дадени упатства. Применувајќи го овој критериум во „набавката на услуги“, клиентот е контролор, бидејќи тој одлучува за целите и начините на обработка, додека пак добавувачот е обработувач, бидејќи постапува според упатствата на контролорот.

Договори за cloud услуги

Кога контролорот користи cloud услуги има обврска да склучи договор со провајдерот на cloud услугите со кој ќе го обврзе провајдерот како обработувач да се усогласи со одредени обврски за заштита на личните податоци. Меѓу другите обврски особено треба да се предвидат следните:

- Предмет, времетраење, природа и цел на обработката, видови на личните податоци кои ќе се обработуваат и категоријата на субјекти на лични податоци;
- Личните податоци ќе бидат обработувани според пишани упатства;
- Вработените лица кај провајдерот коишто се овластени да ги обработуваат личните податоци се имаат обврзано на доверливост;
- Контролорот ќе биде известен за секој планиран подизведувач и ќе има право на приговор;
- Сите подизведувачи се предмет на истите договорни обврски како и обработувачот;
- Соодветни мерки ќе бидат преземени за да се осигура усогласеност на контролорот со неговите законски обврски;
- Сите лични податоци, по прекинот на важење на договорот, ќе бидат избришани или вратени на контролорот; и
- Обработувачот ќе ги направи достапни сите потребни информации и ќе дозволи да се спроведе ревизија за неговото постапување според договорот.

Дополнително, препорачливо е контролорот како клиент да бара:

- Осигурување дека користењето на услугите нема да го стави во позиција на прекршување на неговите законски обврски; и
- Обесштетување во случај на несоодветна обработка на личните податоци од страна на провајдерот како обработувач.

Дисбалансот помеѓу мала компанија корисник на cloud услуги како контролор и голем cloud провајдер како обработувач, не го ослободува контролорот од одговорноста за неисполнување на своите обврски за заштита на личните податоци.[73]

Меѓународен пренос на лични податоци

Несомнено е дека во голем број на случаи cloud технологијата ќе подразбира и меѓународен пренос на лични податоци. Контролорите во cloud околината имаат повеќе опции за да демонстрираат дека при овој пренос се запазени правилата за пренос на лични податоци, како на пример:

- *Географско ограничување* (избор на cloud провајдери од територијата на ЕЕП);
- *Договори за пренос на податоци*;
- *Задолжителни корпоративни правила на обработувачот* (штом овие правила се одобрени од регулаторот, обработувачот добива статус на „безбеден добавувач“);
- *Кодекси на однесување и сертификација;* и
- *Отстапувања во специфични ситуации* (член 53 од Законот за заштита на личните податоци, односно член 49 од Општата регулатива за заштита на личните податоци).

[73] Page 8 from Opinion 05/2012 on Cloud Computing, WP29

Колачиња, слични технологии и IP-адреси

Колачиња (eng. Cookies) се мали текстуални фајлови кои од серверот на посетената веб-страница се пренесуваат на компјутерот на посетителот, и подоцна веб-страницата ќе може да пристапи до нив (на пр. за да идентификува конкретен уред и со тоа да ги запамети log-in деталите и преференциите на посетителот на веб-страницата).

Слични технологии (отпечатоците на уредот) во последните години се развиваат како алтернатива на колачињата што е резултат на ограничената употреба на колачињата на смарт телефоните и другите мобилни уреди.

IP-адреса (Internet Protocol Address) е единствен број доделен на уредот (на пр. компјутер, принтер и сл.) кој на компјутерската мрежа користи интернет за комуникација.

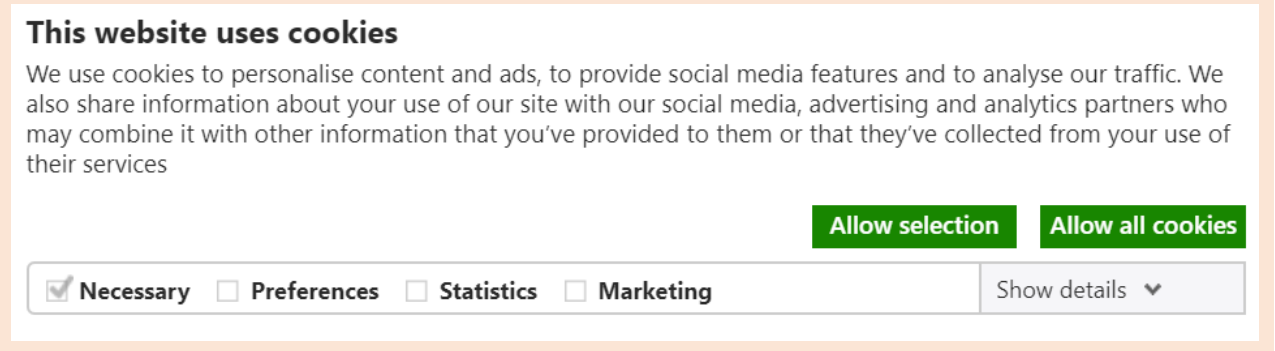
Колачиња и слични технологии како лични податоци

Колачињата и сличните технологии, сами по себе не се лични податоци (на пр. време на посета на веб-страницата). Но, бидејќи со нив може да се идентификува конкретен компјутер, овие податоци може да се користат за да се следи онлајн движење и да се формира профил од пребарувачките навики на конкретниот компјутер, а во голем број на случаи и на физичкото лице зад компјутерот. Иако постојат повеќе мислења, заедничко за сите е дека доколку операторот на веб-страницата може (независно дали има намера) да го поврзе профилот создаден со користење на податоци од колачиња, со име и поштенска/e-mail адреса, тогаш тој профил ќе се смета за личен податок. Кога компанијата користи статичка IP-адресата на физичките лица со цел да креира профил за нив, според Европското тело за заштита на личните податоци, тој профил (вклучувајќи ја и IP-адресата) е личен податок.[74]

Колачиња и согласност

Контролорите коишто обработуваат лични податоци во форма на колачиња имаат обврска пред да го постават колачето на уредот на физичкото лице, од него да добијат информирана согласност. Дополнително, контролорите мора да дадат целосни и точни информации за нивната обработка на колачињата, за што се препорачува донесување посебна Политика за колачиња (Cookies policy).

Пример на барање согласност за користење колачиња:



[74] Page 16 from Opinion 4/2007 on the concept of personal data, WP29

IP-адреси како лични податоци

Исто како колачињата, и IP-адресата може да се користи за креирање профил којшто се смета за личен податок, но за разлика од колачињата, овде се поставува прашањето дали самата IP-адреса е личен податок. Првиот аргумент кој оди во насока да даде потврден одговор на тоа прашање е дефиницијата на личен податок која се повикува на можноста од идентификување конкретно физичко лице, што во овој случај постои затоа што компанијата има можност да креира профил за корисничките пребарувачки навики, па со самото тоа и да го идентификува физичкото лице користејќи ја неговата статичка IP-адреса. Вториот аргумент е дека компанијата може да побара од интернет-сервис провајдерот да го идентификува физичкото лице на кого се однесува IP-адресата и тоа барање да биде реализирано. И двата аргументи ја потврдуваат природата на IP-статичката адресата како личен податок. За динамичките IP-адреси потврда дава Европскиот суд на правдата, според кој динамичките IP се сметаат за лични податоци затоа што и со нив постои можноста од идентификување на одредено физичко лице.[75]

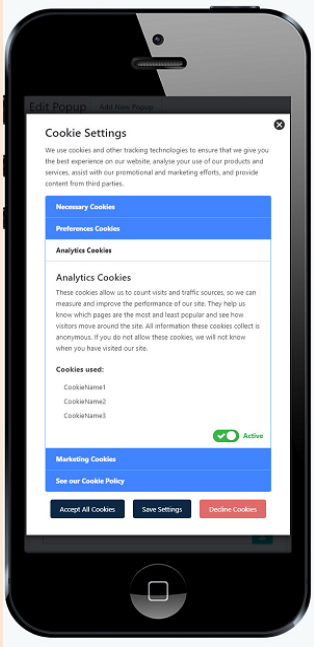
Мобилни апликации

Мобилните апликации собираат голем број на податоци преку сензорите на мобилниот уред каде што се инсталирани (на пр. локација, аудио, фотографии, именик, и сл.). Сето тоа наведува дека мобилните апликации може да обработуваат голема количина на лични податоци за сопственикот на мобилниот уред, кои понатаму може да се користат за попрецизно креирање кориснички профили со примена на профилирањето како метод.

Колачиња и слични технологии

Доколку мобилната апликација користи колачиња или слични технологии, во тој случај се применуваат правилата за заштита на личните податоци.

Известување



Како резултат на малиот екран на мобилните уреди, класичните политики за приватност не секогаш ќе бидат соодветни за да се задоволат обврските од принципот на транспарентност. Европското тело за заштита на личните податоци препорачува користење икони или други слични визуелни означувања како корисна алатка за подобро донесување на информациите до корисникот. А за да се задоволи барањето информациите да бидат дадени пред обработка на личните податоци, известувањето може да се даде пред мобилната апликација да биде симната (на пр. политика за приватност објавена во App Store).

[75] Patrick Breyer v. Germany 2016, Case C-582/14, 12.05.2016

Согласност за обработка на личните податоци преку мобилна апликација

Според високите стандарди кои се поставени за една согласност да се смета за валидна, развивачите на апликации се соочени со многу предизвици. Согласност за обработката на личните податоци која не е неопходна за функционирање на мобилната апликација генерално нема да се смета за валидна доколку корисникот морал да ја даде за да ја користи апликацијата, од причина што би се сметала за условена согласност. Исто така, за да се задоволи епитетот „конкретна" треба да му се даде на корисникот можност посебно да се согласи за секоја одделна обработка на личните податоци, наместо да даде една генерална согласност за сите видови на обработка. Во практична смисла тоа би значело барање на посебни согласности од корисниците за секој посебен вид на обработка на нивните лични податоци и овозможување колку што може повеќе функционалности доколку корисникот не даде одредена согласност.

Минимална количина на податоци

Со примена на принципот на заштита на личните податоци by default, развивачите на мобилните апликации мора да осигураат дека ќе се обработуваат само неопходните, релевантните и соодветните лични податоци.

Internet Of Things (IoT)

IoT се објекти кои се поврзани на интернет и кои може да комуницираат со други објекти поврзани на интернет без помош од страна на човек. Во многу случаи, овие објекти содржат сензори кои собираат и пренесуваат информации за нивната околина, односно за „...физички лица кои можат да се идентификуваат".[76]

Безбедност

Барањето за примена на соодветни безбедносни мерки за пренос на личните податоци преку мрежите на коишто се прикачени IoT објектите претставува предизвик, особено поради:

- Големиот број на објекти коишто често се поврзани на истата мрежа, овозможувајќи голем број на точки преку кои непријателски актери може да добијат пристап до мрежата;
- Малата веројатност дека софтверот на IoT објектите редовно е надградуван со најновите безбедносни закрпи.

[76] Член 4, став (1), точка 1 од Законот за заштита на личните податоци „(Сл. весник на РСМ" број 42 од 16.2.2020 година)

Известување и избор

Известувањето и согласноста претставуваат дополнителен предизвик затоа што при собирањето и обработката на личните податоци од страна на IoT објектите нема човечка активност. Треба да се размисли на кој начин физичките лица чии лични податоци се обработуваат од страна на IoT објектите, ќе се информираат со деталите за обработката. Неспорно е дека решенијата за овој предизвик ќе зависат од конкретната технологија и ќе бараат иновативни пристапи.

Opinion on Cloud Computing, WP29;
Opinion on the concept of personal data, WP29.

13. Outsourcing[77]

Во најголем број на случаи кога станува збор за outsourcing, улогите се поделени така што клиентот е контролор, а outsourcing компанијата е обработувачот. Поделбата на овие улоги е значајна за соодветна примена на обврските и одговорностите кои произлегуваат за секоја страна.

Одредби за заштита на личните податоци во договорите за outsourcing

Обработка согласно упатствата на контролорот

За прецизна дистинкција помеѓу улогите на контролор (т.е. клиент) и обработувач (т.е. добавувач), од особено значење е во договорот за outsourcing кој предвидува обработка на лични податоци да се наведе кој е кој. Исто така, договорот треба да ја вклучува одредбата дека добавувачот ќе ги обработува личните податоци само според документирани упатства добиени од страна на клиентот.

Примена на соодветни технички и организациски мерки

Ова исто така претставува една од основните законски обврски, и во одредени сценарија можеби би било мудро контролорите да се потпрат на експертизата на добавувачот да процени кои безбедносни мерки ќе бидат имплементирани, и притоа да се наведе во договорот:

- дека клиентот ќе се потпре на способностите и знаењето на добавувачот да процени со кои „соодветни мерки“ за да ги заштити личните податоци од неовластена или незаконска обработка, губење, откривање, и слично,
- дека техничките и организациските мерки мора да бидат соодветни на повредата што може да настане како резултат на некоја неовластена или незаконска обработка, губење, откривање и слично.

[77] Ова поглавје се однесува и на примената на Законот за заштита на личните податоци, но и на примената на Општата регулатива за заштита на личните податоци на македонските компании кои нудат outsourcing услуги на компании во ЕУ

Дополнително, од добавувачот може да биде побарано да ја земе предвид:

- чувствителната природа на личните податоци и
- состојбата на технолошкиот развој на трошоците на имплементација на таквите мерки.

Проверка на вработените лица кај добавувачот

Како дел од организациските безбедносни мерки е и проверката (ветинг) на вработените лица. Стана честа пракса во договорите да се вметнуваат конкретни обврски за добавувачите кои се однесуваат на доверливоста на нивните вработени или вработените на подизведувачите. Со овие обврски може да се бара од добавувачите:

- да ја осигураат доверливоста на секој вработен и вработените на подизведувачите кои имаат пристап до личните податоци на клиентот,
- сите вработени и вработените на подизведувачите кои вршат обработка на личните податоци на клиентот имаат посетено соодветна обука за заштита на личните податоци и
- дека сите вработени и вработените на подизведувачите ќе ги вршат своите обврски исклучиво во согласност со соодветните договорни одредби за доверливост.

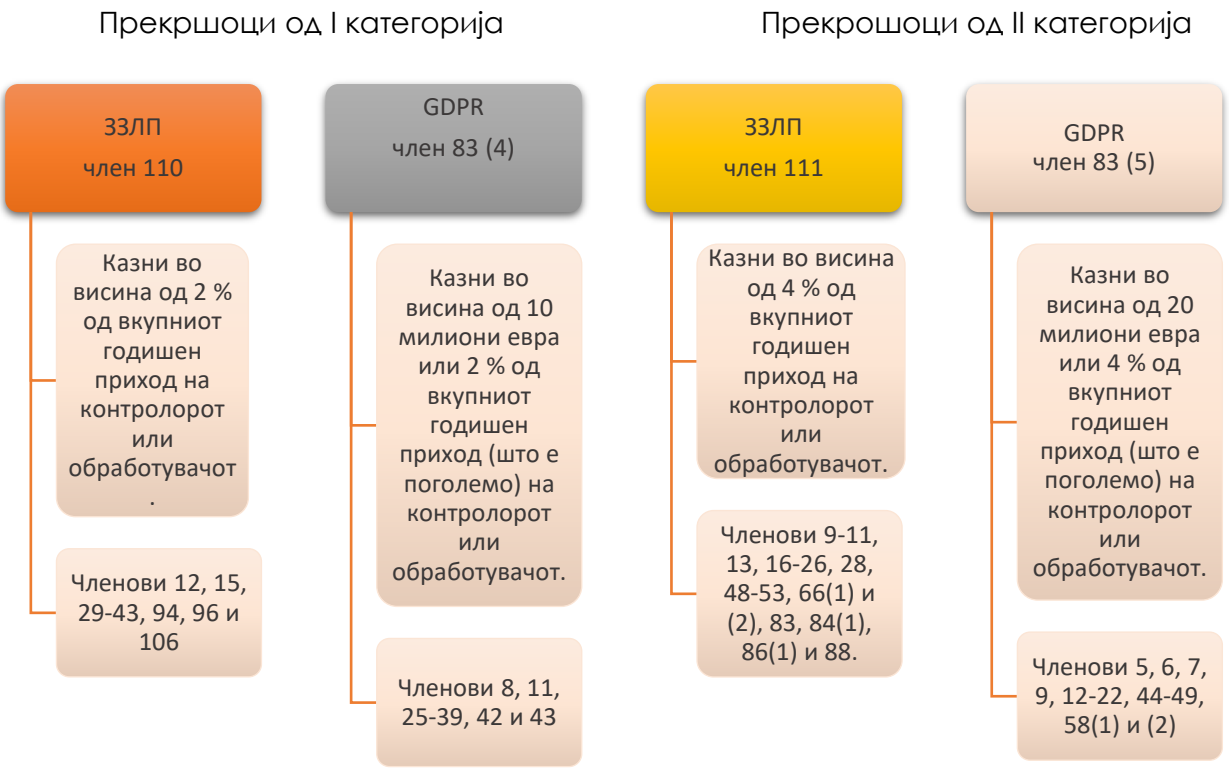
14. Регулација и прекршоци

Со новата регулативата за заштита на личните податоци, регулацијата се поставува на повеќе нивоа, а не само во рацете на регулаторот – Агенцијата за заштита на личните податоци. Имено, моќта на регулатор им се дава на судовите, на пазарот, на саморегулацијата и, се разбира, на субјектите на личните податоци.

Прекршоци

Висината на казните предвидени со регулативата за заштита на личните податоци е она што ја постави оваа регулатива во центарот на вниманието. Сведоци сме на огромни изречени казни за светски компании поради нивна неусогласеност со Општата регулатива за заштита на личните податоци, од кои досега највисоката изречена казна е дури 204 милиони евра.[78]

Разлика се јавува и во постоењето на посебната одредба за прекршоци сторени при вршење видеонадзор[79] коишто законот ги издвојува како посебна категорија на прекршоци, а таква одредба не постои во Општата регулатива за заштита на личните податоци.



15. Заклучок

Компаниите за коишто е применлив Законот за заштита на личните податоци мора да бидат свесни за законските барања кои ги засегаат, и со тие барања да се усогласат најдоцна до август 2021 година. Законот за заштита на личните податоци, а воедно и Општата регулатива за заштита на личните податоци, не прават разлика помеѓу видовите на компаниите, нивната големина, индустријата на која припаѓаат и слично, туку единствен важен параметар е дали има процеси на обработка на личните податоци. Па така, во компанија со неколкумина вработени може да има голем број на процеси на обработка

[78] Изречена од Information Commissioner (ICO) на British Airways поради неусогласеност со членот 32 од GDPR (Security of processing)

[79] Член 112 од Законот за заштита на личните податоци („Сл. весник на РСМ“ број 42 од 16.2.2020 година)

на лични податоци (на пр. стоматолошка ординација), и обратно, во компанија со голем број на вработени да има само неколку процеси на обработка на лични податоци (на пр. фабрика за производство на акумулатори). И двете компании, мора да ги преземат сите обврски и одговорности за да ги усогласат своите процеси на обработка на личните податоци со правилата за заштита на личните податоци.

Исто така, не постои официјално дефинирана патека по којашто една компанија треба да се движи за да се усогласи со Законот за заштита на личните податоци (и/или Општата регулатива за заштита на личните податоци). Сепак, водејќи се од европската пракса и од препораките на регулаторите и телата за заштита на личните податоци, во прилог е дадена предлог-листа со чекори кои една компанијата (независно од големината, индустријата и сл.) би можеле да ја доведат до целта – усогласеност со регулативата за заштита на личните податоци.

16. Патека до усогласеност со Законот за заштита на личните податоци