

Формуляр за частична предварителна оценка на въздействието* (Приложете към формуляра допълнителна информация/документи)	
Институция: МВР	Нормативен акт: проект на Закон за изменение и допълнение на Закона за защита на личните данни (обн. ДВ. бр.1 от 2002 г., изм. ДВ. бр.70 от 2004 г., изм. ДВ. бр.93 от 2004 г., изм. ДВ. бр.43 от 2005 г., изм. ДВ. бр.103 от 2005 г., изм. ДВ. бр.30 от 2006 г., изм. ДВ. бр.91 от 2006 г., изм. ДВ. бр.57 от 2007 г., изм. ДВ. бр.42 от 2009 г., изм. ДВ. бр.94 от 2010 г., изм. ДВ. бр.97 от 2010 г., изм. ДВ. бр.39 от 2011 г., изм. ДВ. бр.81 от 2011 г., изм. ДВ. бр.105 от 2011 г., изм. и доп. ДВ. бр.15 от 2013 г., доп. ДВ. бр.81 от 2016 г., изм. ДВ. бр.7 от 19.01.2018 г.)
За включване в законодателната/оперативната програма на Министерския съвет за периода:	Дата: законопроектът не е включен в законодателната програма на МС.
Контакт за въпроси: Мария Рангелова – началник сектор „Международно-правни въпроси“ в дирекция „ЕС и международно сътрудничество“ – МВР mrangelova.14@mvr.bg Иван Александров – главен юрисконсулт в сектор „Международно-правни въпроси“ на дирекция „ЕС и международно сътрудничество“ – МВР Imaleksandrov.14@mvr.bg	Телефони: 982 21 14 982 28 94
1. Дефиниране на проблема: 1.1. Кратко опишете проблема и причините за неговото възникване. Посочете аргументите, които обосновават нормативната промяна. През януари 2012 г. Европейската комисия предложи цялостна реформа в областта на защитата на личните данни, състояща се от два законодателни документа: Общ регламент за защита на личните данни и Директива за обработването на лични данни в сектора полиция и правосъдие. След 4-годишни преговори, на 4 май 2016 г. в Официален вестник на Европейския съюз бяха обнародвани Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните) и Директива (ЕС) 2016/680 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни от компетентните органи за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания и относно свободното движение на такива данни, и за отмяна на Рамково решение 2008/977/ПВР на Съвета. Предлаганата нормативна промяна (проект на Закон за изменение и допълнение на Закона за защита на личните данни) е продиктувана от следните обстоятелства: • С обнародването на европейския законодателен пакет е финализирана европейската реформа за защита на личните данни, основна цел на която е да се модернизират действащите правила за защита на данните с оглед на бързото развитие на технологиите и глобализацията. • Необходимо е транспониране на разпоредбите на Директивата за обработването на лични данни в сектора полиция и правосъдие. Срокът за транспонирането ѝ е 6 май 2018 г. • Въпреки подробната и цялостна уредба на защитата на личните данни в регламента и независимо от прякото му действие, е необходимо на национално ниво да бъдат въведени мерки за неговото изпълнение – както по отношение	

отделни негови разпоредби, които изрично изискват национална правна уредба, така и по отношение въпроси, по които регламентът предоставя възможност за избор на държавите-членки.

1.2. Опишете какви са проблемите в прилагането на съществуващото законодателство или възникналите обстоятелства, които налагат приемането на ново законодателство. Посочете възможно ли е проблемът да се реши в рамките на съществуващото законодателство чрез промяна в организацията на работа и/или чрез въвеждане на нови технологични възможности (например съвместни инспекции между няколко органа и др.).

С оглед завишените стандарти в областта на защитата на личните данни на ниво Европейски съюз (ЕС), запазването на част от действащото законодателство без промяна ще доведе до явно несъответствие на редица ключови въпроси с новите правила, произтичащи от Регламент 2016/679 и Директива 2016/780. Европейският законодателен пакет въвежда множество нови изисквания към всички заинтересовани страни: администратори на лични данни, обработващи лични данни, субекти на данни и национални надзорни органи по защита на данните, както следва:

- Разширен е значително понятиятният апарат в областта на защитата на личните данни и са разписани подробни правни дефиниции;
- Разширен е обхватът на принципите за защита на личните данни и е обогатено тяхното съдържание;
- Разширени са изискванията към администраторите на лични данни за предварително консултиране с надзорния орган;
- Въведени са конкретни изисквания към обработването на лични данни за друга цел, различна от първоначалната, за която данните са били събрани;
- Завишени са изискванията към администраторите на лични данни, в случаите, в които обработването на данни се основава единствено на съгласие на субекта на данни;
- Отделено е специално внимание на обработването на лични данни на деца и са въведени изисквания за удостоверяване даването на съгласие от страна на дете във връзка с използването на услуги на информационното общество;
- Разширен е обхватът на хипотезите, при които е допустимо обработване на специални категории данни;
- Разширен е значително кръгът от права на субектите на данни и механизми за тяхната защита, включително правото да бъдеш забравен;
- Отпада административната тежест за извършване на регистрация на администраторите на лични данни преди започване обработването на данни, като едновременно с това значително е разширен кръгът от задължения на администраторите и обработващите;
- Разширени са значително задачите и правомощията на надзорните органи за защита на данните (за Република България такъв орган е Комисията за защита на личните данни), вкл. правомощия за разследване, корективни правомощия и правомощия за даване на разрешения и становища;
- Въвежда се фигурата на длъжностното лице по защита на данните и се разписват хипотезите, при които определянето на такъв служител е задължително при администраторите на лични данни;
- Въвежда се услуга на едно гише за администраторите на лични данни;
- Въвежда се механизъм за сертифициране за защита на личните данни;
- Значително се увеличават правните инструменти, посредством които администратори и обработващи могат да предават лични данни към трети държави – т.нар. трансфери на данни;
- За първи път е въведен механизъм на съгласуваност и сътрудничество между надзорните органи за защита на данните, вкл. осъществяване на съвместни операции;
- Институционализира се Европейски комитет по защита на данните с възможност за даване на задължителни становища до националните надзорни органи;
- Значително се завишават размерите на административните наказания „глоба“ или „имуществена санкция“ за нарушения на правилата за защита на данните;
- Допуска се въвеждането на особени правила при обработването на лични данни в трудовия контекст, за целите на свободата на изразяване и информация; обработването на национален идентификационен номер и др.
- Установява се детайлен правен режим при обработването на лични данни за целите

на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания, включително предпазването от заплахи за общественения ред и сигурност и тяхното предотвратяване.

Прилагането на по-горе посочените изисквания в областта на защитата на личните данни не може да се гарантира посредством приемането на промяна в организацията на работа и/или чрез въвеждане на нови технологични възможности. Въпреки пряката приложимост на регламента, множество от посочените нови правила налагат въвеждането на национална правна регламентация, която да осигури необходимите предпоставки за реализацията им спрямо всички заинтересовани страни. В допълнение следва да се има предвид, че нормите на Директивата следва задължително да бъдат въведени в българското законодателство поради липсата на пряко действие на този правен акт на ЕС в държавите членки.

1.3. Посочете дали са извършени последващи оценки на нормативния акт, или анализи за изпълнението на политиката и какви са резултатите от тях?

Последваща оценка на въздействието не е извършвана.

2. Цели:

Основната непосредствена цел на предлаганите изменения и допълнения в Закона за защита на личните данни е предприемането на мерки по изпълнението на Регламент 2016/679 и въвеждането в националното законодателство на изискванията на Директива 2016/680. По този начин се гарантира постигането и на следните стратегически цели:

- Да се повиши ефективността на прилагането на основното право на защита на личните данни в Република България (чл. 8 от Харта на основните права на Европейския съюз и чл. 16 от ДФЕС) и да се гарантира, че физическите лица имат контрол върху своите данни;
- Да се постигне всеобхватна и задълбочена синхронизация на националната правна рамка с европейското законодателство за защита на личните данни;
- Да се гарантира съгласуваността на правната рамка на национално ниво в областта на защитата на данните;
- Да се намали административната тежест за администраторите на лични данни;
- Да се усъвършенстват специалните правила за защита на физическите лица във връзка с обработването на лични данни от компетентните органи за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления, или изпълнението на наказания, включително предпазването от заплахи за обществената сигурност и тяхното предотвратяване, като се отчита специфичният характер на тези дейности;
- Да се осигури свободното движение на лични данни между държавите членки на ЕС, при което се обезпечава хомогенно и високо ниво на защита на личните данни на физическите лица и улесняването на обмена на лични данни между компетентните органи на държавите членки.

Целите, които си поставя нормативната промяна напълно съответстват на действащата стратегическа рамка. Тези цели са заложили и в приетата през 2017 г. Стратегия на КЗЛД за развитие в областта на защитата на личните данни (Хоризонт 2022). От своя страна стратегията е съобразена с Националната програма за развитие: България 2020 и Стратегията за развитие на държавната администрация (2014 – 2020), като по този начин се осигурява съответствие с националната стратегическа рамка, която е с надсекторен обхват.

Посочете целите, които си поставя нормативната промяна, по конкретен и измерим начин и график, ако е приложимо, за тяхното постигане. Съответстват ли целите на действащата стратегическа рамка?

3. Идентифициране на заинтересованите страни:

Преки заинтересовани страни:

1. Комисията за защита на личните данни в качеството ѝ на национален надзорен орган по защита на данните;

2. Администратори на лични данни в публичния, частния и неправителствения сектор – такива са всяко физическо или юридическо лице, както и орган на държавната власт или на местното самоуправление, публичен орган или друго образувание или структура, който сам или съвместно с друго лице определя целите и средствата за обработване на личните данни, или чиито цели и средства за обработване са определени в закон;

3. Обработващи лични данни в публичния, частния и неправителствения сектор - такива са всяко физическо или юридическо лице, държавен орган или орган на местно самоуправление,

който обработва лични данни от името на администратор на лични данни;

4. Публични органи, компетентни за предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания, като структури на Министерството на вътрешните работи, прокуратура, съд, структури на Министерството на правосъдието, ДАНС, Агенция „Митници“;

5. Физическите лица, независимо от тяхното гражданство и местопребиваване, чиито лични данни са обект на обработване от администратори и обработващи лични данни.

Косвени заинтересовани страни: няма.

Посочете всички потенциални засегнати и заинтересовани страни, върху които предложението ще окаже пряко или косвено въздействие (бизнес в дадена област/всички предприемачи, неправителствени организации, граждани/техни представители, държавни органи, др.).

4. Варианти на действие:

Вариант на действие 1 – „Без действие“

Този вариант на действие е недопустим, тъй като при него ще се стигне до:

- Липса на каквито и да било мерки на национално ниво, с които да бъдат въведени нормите на директивата и предприемането на мерки по изпълнение на Регламента;
- Прилагане по неправилен начин на разпоредби от европейското право;
- Неправилно функциониране на системата за защита на личните данни;
- Правна несигурност в областта на защитата на личните данни в Република България;
- Стартиране на процедура срещу Република България от страна на Европейската комисия по чл. 258 - 260 от Договора за функционирането на ЕС (иск за установяване на неизпълнение на задълженията от държава-членка).

Вариант на действие 2 – „Два самостоятелни закона – общ и специален“: „Закон за изменение и допълнение на Закона за защита на личните данни“ и „Закон за защита на личните данни за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания, включително предпазването от заплахи за обществения ред и сигурност и тяхното предотвратяване“

Този вариант на действие е допустим, тъй като при него ще се стигне до въвеждане на мерките по изпълнение на Регламент 2016/679 и транспонирането на изискванията на Директива 2016/680. Последните ще бъдат въведени в националното законодателство с два самостоятелни закона, както следва:

- Със Закона за изменение и допълнение на Закона за защита на личните данни ще бъдат въведени мерки на национално ниво, които да гарантират приложението на Регламент 2016/679;
- Със Закон за защита на личните данни за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания, включително предпазването от заплахи за обществения ред и сигурност и тяхното предотвратяване ще бъде транспонирана Директива 2016/780.

При този вариант на действие обаче има опасност от ненужна фрагментарност на правната уредба в областта на защитата на личните данни на национално ниво и евентуална несъгласуваност между двата нормативни акта.

Вариант 3 – „Закон за изменение и допълнение на Закона за защита на личните данни“

Този вариант на действие е допустим и предпочитан, тъй като при него ще се постигне:

- Съответствие с нормативните изисквания на Закона за нормативните актове - при наличие на нормативна уредба на дадена материя в закон, да се прави изменение и допълнение в този закон, а не нов закон;
- Кодифициране на правната материя в областта на защитата на личните данни;
- Ще се въведат норми в националното законодателство, които съответстват на европейското право;
- Функционирането на националната система за защита на личните данни ще бъде надградена и ще се синхронизира с европейската правна рамка, при запазване на единния надзорен орган;
- Ще се гарантира правна сигурност за администраторите на лични данни,

обработващите и субектите на данни;

- Облекчено правоприлагане поради опростяване на регулаторната рамка. .

Във връзка с този вариант на действие, който е предпочитан, проектът на Закон за изменение и допълнение на Закона за защита на личните данни въвежда следните промени:

1. Въвеждат се мерки за изпълнение на Общия регламент, като:

- ❖ се актуализират правомощията на Комисията за защита на личните данни с цел да се отговори на разширения обхват от задачи и функции на надзорните органи, произтичащи от чл. 57 и чл. 58 от Общия регламент;
- ❖ се въвежда принципът, че съдилищата са изключени от надзора на Комисията за защита на личните данни, когато обработват лични данни при изпълнение на съдебните им функции;
- ❖ Комисията за защита на личните данни се определя като орган, компетентен да акредитира сертифициращи органи в областта на защитата на личните данни;
- ❖ регламентира се поддържането на публични и непублични регистри, поддържани от Комисията за защита на личните данни в изпълнение на засилените й правомощия по Общия регламент;
- ❖ разписват се т.нар. особени ситуации за обработване на лични данни, като баланса между правото на защита на личните данни и свободата на изразяване и информация, обработване на единен граждански номер, обработване на лични данни в трудовия контекст, обработване на данни чрез средства за видеонаблюдение, обработване на лични данни на починали лица;
- ❖ въвеждат се два нови режима - режим на акредитиране на сертифициращи органи и режим на сертифициране, И двата режима са доброволни, като проекта на закон не предвижда такси за прилагането им. За нарушения на задълженията на администратор или обработващ, произтичащи от дейността по сертифицирането, Общият регламент (а не проекта на Закон за изменение и допълнение на Закона за защита на личните данни) предвижда носене на административно-наказателна отговорност в размер до 10 000 000 евро или до 2% от общия годишен световен оборот на съответния администратор/обработващ.

2. Транспонират се разпоредбите на Директивата за обработването на лични данни в сектора полиция и правосъдие.

Идентифицирайте основните регулаторни и нерегулаторни възможни варианти на действие от страна на държавата, включително варианта "без действие".

5. Негативни въздействия:

Вариант за действие 1 – „Без действие“

Няма да бъдат предприети задължителните нормативни промени, с които да се синхронизира националната правна уредба с новите стандарти за защита на данните, въведени със законодателния пакет на ЕС през 2016 г. Прибягването до този вариант ще доведе до следните значителни негативни въздействия върху всички заинтересовани страни – администратори, обработващи, субекти на данни, компетентни органи, КЗЛД:

- **Икономически негативни въздействия:** Липсата на каквито и да било действия по транспониране ще създаде пречки пред изграждането на пространство на свобода, сигурност и правосъдие и на постигането на икономически и социален напредък. В допълнение, ще доведе до откриване на наказателна процедура от Европейската комисия срещу страната ни за невъвеждане на мерките по изпълнение на Регламент 2016/679 и на Директива 2016/680, респ. до негативно финансово въздействие върху държавния бюджет.

- **Социални негативни въздействия:** Субектите на данни ще бъдат лишени от възможността да се позоват и да упражнят реално правата си в областта на защитата на личните данни, вкл. при обработване на лични данни за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания, включително предпазването от заплахи за обществен ред и сигурност и тяхното предотвратяване. Администраторите и обработващите данни няма да реализират значителен обем от задълженията си, което ще доведе до правна несигурност в

цялата система за защита на личните данни. Комисията за защита на личните данни няма да отговори на нормативните изисквания за независимост на надзорния орган и няма да може да гарантира реализирането на основното право на гражданите на защита на личните им данни.

- **Екологични негативни въздействия:** не може да има.

Вариант за действие 2 - „Два самостоятелни закона – общ и специален“

При този вариант на действие предметът на правната уредба на двата самостоятелни закона ще бъде идентичен - „обработване и защита на лични данни“. Фактът, че целите, за които данните се обработват и субектите, които ги обработват, са различни, респ. имат различен източник от правото на ЕС, не променя обстоятелството, че става въпрос за обществени отношения от една и съща област. Затова, в случай че се прибегне до този вариант, няма да бъдат изпълнени изискванията на чл. 10 от Закона за нормативните актове, съгласно който обществените отношения от една и съща област следва да се уреждат с един, а не с няколко нормативни актове от същата степен.

- **Икономически негативни въздействия:** не може да има.
- **Социални негативни въздействия:** ще доведе до правна несигурност за всички заинтересовани страни.

Администраторите на лични данни и обработващите данни в сектора полиция и правосъдие ще следва да прилагат два самостоятелни правни режима в зависимост от качеството, в което действат:

Да прилагат общия закон за всички дейности по обработване, които не са свързани с предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания, включително предпазването от заплахи за обществения ред и сигурност и тяхното предотвратяване;

Да прилагат само специалния закон винаги, когато дейностите по обработване са за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания, включително предпазването от заплахи за обществения ред и сигурност и тяхното предотвратяване.

По аналогичен начин, субектите на данни ще бъдат значително затруднени в преценката си дали при упражняването на правата си в областта на защитата на личните данни следва да се позовават на общия или на специалния закон.

Нецелесъобразно и недопустимо е да се очаква, че субектите на данни и/или администраторите са в състояние да правят правна преценка относно приложимото законодателство с цел упражняване на своите права, респ. изпълнение на своите задължения.

Затрудненията, които биха изпитали заинтересованите страни – администратори и обработващи в сектора полиция и правосъдие ще доведе до повишаване броя на жалби и сигнали за неправомерно обработване на лични данни, респ. до засилено сезиране на Комисията за защита на личните данни, която във всеки конкретен случай ще следва да преценява целите за обработване на данни, за да може да бъде индивидуализирано приложимото правно основание.

Администраторите и обработващите извън сектора полиция и правосъдие няма да изпитват затруднения в процеса на правоприлагане, тъй като за тях ще се прилага единствено общият режим – този по Закона за защита на личните данни. В този смисъл за тях не се очаква да възникнат социални негативни въздействия.

- **Екологични негативни въздействия:** не може да има.

Вариант 3 – „Закон за изменение и допълнение на Закона за защита на личните данни“

При този вариант няма негативни въздействия върху заинтересованите страни.

- **Икономически негативни въздействия:** не може да има
- **Социални негативни въздействия:** не може да има
- **Екологични негативни въздействия:** не може да има.

Опишете качествено (при възможност - и количествено) всички значителни

потенциални икономически, социални, екологични и други негативни въздействия за всеки един от вариантите, в т.ч. разходи (негативни въздействия) за идентифицираните заинтересовани страни в резултат на предприемане на действията. Пояснете кои разходи (негативни въздействия) се очаква да бъдат второстепенни и кои да са значителни.

6. Положителни въздействия

Вариант за действие 1- „Без действие“

При този вариант на действие не са идентифицирани положителни въздействия за нито една от заинтересованите страни.

Вариант за действие 2- „Два самостоятелни закона – общ и специален“

При този вариант за действие единственото положително въздействие е, че ясно ще бъдат разграничени на национално ниво правните актове, с които са предприети мерки по изпълнение на Регламент 2016/679 и Директива 2016/680. Това би улеснило процеса по докладване до Европейската комисия, тъй като двата закона на национално ниво – общ и специален, ще съответстват напълно по предмет и обхват на двата европейски акта, чиито норми те въвеждат. С изключение на Комисията за защита на личните данни, която е компетентният национален орган в областта на защитата на данните, този вариант за действие не води до никакви положителни въздействия върху останалите заинтересовани страни. Положителното въздействие върху КЗЛД се свежда единствено до въвеждането на изчерпателна национална правна уредба на горепосочените два европейски акта.

- **Икономически положителни въздействия:** липса на наказателна процедура срещу Република България.
- **Социални положителни въздействия:** не може да има.
- **Екологични положителни въздействия:** не може да има.

Вариант за действие 3 - „Закон за изменение и допълнение на Закона за защита на личните данни“

• **Икономически положителни въздействия:** създаване на условия за изграждане на пространство на свобода, сигурност и правосъдие и постигане на икономически и социален напредък, укрепване и сближаване на икономиките в рамките на единния вътрешен пазар. Липса на наказателна процедура срещу Република България. Това положително въздействие се очаква да има проявление спрямо всички заинтересовани страни – администратори, обработващи, субекти на данни, компетентни органи в сектора полиция и правосъдие, Комисия за защита на личните данни, тъй като всички тези страни ще прилагат унифицирани правила и изисквания в областта на защитата на личните данни.

• **Социални положителни въздействия:** Правилно прилагане на изискванията на чл. 10 от Закона за нормативните актове, тъй като обществените отношения от една и съща област ще бъдат уредени с един, а не с няколко нормативни актове от същата степен. Това ще гарантира правна сигурност сред всички заинтересовани страни.

- **Екологични положителни въздействия:** не може да има.

Опишете качествено (при възможност - и количествено) всички значителни потенциални икономически, социални, екологични и други ползи за идентифицираните заинтересовани страни за всеки един от вариантите в резултат на предприемане на действията. Посочете как очакваните ползи кореспондират с формулираните цели.

7. Потенциални рискове:

Вариант за действие 1- „Без действие“

Основните рискове при този вариант са:

- липсата на каквито и да било мерки на национално ниво, с които да се въведат разпоредбите на Директива 2016/680 и да се предприемат мерки по изпълнението на Регламент 2016/680.
- стартирането на наказателна процедура срещу Република България от страна на Европейската комисия по чл. 258 - 260 от Договора за функционирането на ЕС.

Вариант за действие 2- „Два самостоятелни закона – общ и специален“

Основните рискове при този вариант са:

- фрагментарност на правната уредба и/или непълно и/или неправилно транспониране на европейското право;
- правна несигурност сред администраторите на лични данни, обработващите лични данни и субектите на данни;
- неправилно определяне на приложимото право, респ. значително увеличаване на случаите на нарушения при обработването на лични данни и затруднено правоприлагане.

Вариант за действие 3—„Закон за изменение и допълнение на Закона за защита на личните данни“

Не са идентифицирани конкретни рискове при реализирането на този вариант.

Общо за варианти 2 и 3:

С оглед на обстоятелството, че при тези два варианта се очакват нови аспекти в националната правна уредба, потенциални рискове са:

- приемане на нормативните промени след крайния срок, предвиден по Регламент 2016/679 – 25 май 2018 г. и Директива 2016/680 – 6 май 2018 г.;
- трудно ориентиране в новите и завишени изисквания в областта на защитата на личните данни, произтичащи от новата правна уредба от страна на администратори, обработващи и субекти на данни;
- недостиг на финансови и човешки ресурси на КЗЛД за изпълнение на новите задачи и правомощия;
- липса на финансиране по бюджета на КЗЛД за обезпечаване функционирането на обучителен център в областта на защитата на личните данни, който да отговори на нарасналата потребност от информиране на обществото по ключови въпроси, свързани със защитата на данните.

Посочете възможните рискове от приемането на нормативната промяна, включително възникване на съдебни спорове.

8.1. Административната тежест за физическите и юридическите лица:

- ☐ Ще се повиши
☐ **Ще се намали**
☐ Няма ефект

Административната тежест на администраторите на лични данни (от публичния, частния и неправителствения сектор) намалява, тъй като отпада задължението им за регистрация в КЗЛД. Въпреки че регистрацията е безплатна и достъпна онлайн, тя е ресурсоемка дейност, неизпълнението на която е скрепено с носене на административно-наказателна отговорност по досега действащата правна уредба. Допълнително облекчение от отпадането на регистрационния режим ще усетят най-вече администраторите, които обработват т.нар. чувствителни данни (данни, разкриващи расов или етнически произход, политически, религиозни или философски убеждения, данни, отнасящи се до здравето, сексуалния живот или до човешкия геном), тъй като техният процес на регистрация досега беше допълнително усложнен с извършването на предварителна проверка.

8.2. Създават ли се нови регулаторни режими? Засягат ли се съществуващи режими и услуги?

Създават се два нови режима:

- режим на акредитиране на сертифициращи органи. Предвижда се акредитацията да бъде извършвана от КЗЛД.
- режим на сертифициране, чиято цел е да се демонстрира спазване на изискванията в областта на защитата на личните данни. Сертифицирането е доброволно на основание чл. 42, пар. 3 от Регламент 2016/679.

По принцип създаването на тези два нови режима няма да доведе до допълнителна административна тежест, тъй като те са доброволни. Доколкото обаче Общият регламент изисква акредитирането да става по критерии, определени от надзорният орган (Комисията за защита на личните данни), а сертифициращите органи да отговарят на определени изисквания, то режима на акредитиране ще има определени въздействия върху организациите, кандидатстващи за статут на сертифициращи органи. Последните ще следят за съответствието на

администраторите, избрали да бъдат обект на сертифициране, с изискванията за защита на личните данни.

По отношение режима на сертифициране следва да се има предвид, че администраторите и обработващите – обект на сертифициране, на практика ще трябва да доказват, че изпълняват изискванията на Общия регламент за защита на данните, т.е. за тях не се очаква да възниква допълнителна административна тежест, различна от общите задължения в областта на защитата на личните данни.

Засягат се два съществуващи режима:

- режим на регистрация на администраторите на лични данни. С влизането в сила на Регламент 2016/679 регистрацията отпада, поради което е предвидено съответните текстове в ЗЗЛД, касаещи този процес, да бъдат отменени. Това намалява административната тежест на администраторите на лични данни.

- режим на разрешаване предаването на данни към трети държави. Регламент 2016/679 значително разширява кръга от правни инструменти за трансфер на лични данни, като по този начин облекчава дейността на администраторите и обработващите данни. В проекта на Закон за изменение и допълнение на ЗЗЛД се предвижда глава шеста, която урежда предоставяне на лични данни на трети лица, да бъде отменена. Специалните правила, свързани с трансфера на данни за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания, включително предпазването от заплахи за обществения ред и сигурност и тяхното предотвратяване, са предмет на изчерпателна уредба в проекта на ЗИДЗЗЛД с цел транспониране на Директива 2016/680.

9. Създават ли се нови регистри?

Създават се два типа регистри:

- регистри, поддържани от КЗЛД, както следва:

1. публичен регистър на длъжностните лица по защита на данните;
2. публичен регистър на кодекси за поведение;
3. публичен регистър на акредитираните сертифициращи органи;
4. вътрешен регистър на нарушения на Регламент 2016/679 и на ЗЗЛД, както и на

предприетите мерки в съответствие с упражняването на корективните правомощия на Комисията за защита на личните данни.

- регистър на дейностите по обработване на лични данни, поддържан от администраторите на лични данни и обработващите. Тези регистри следва да се поддържат в писмена форма, вкл. в електронен формат. Точният брой е променлива величина с оглед променливия брой на администраторите на лични данни, предмета им на дейност и категориите данни – обект на обработване. Задължението за поддържане на тези регистри възниква при условията на чл. 30 от Регламент 2016/679.

Когато отговорът е "да", посочете колко и кои са те

10. Как въздейства актът върху микро-, малките и средните предприятия (МСП)?

☐ **Актът засяга пряко МСП** – ЗИДЗЗЛД въвежда общо задължение при прилагането на закона да бъдат отчитани специфичните потребности на микро-, малките и средни предприятия при условията на Регламент 2016/679. Регламентът предвижда облекчения за тях при поддържането на регистри на дейностите по обработване на лични данни, при изготвяне на кодекси за поведение и механизмите за сертифициране, както и при повишаването на информираността им по въпроси в областта на защитата на личните данни.

☐ Актът не засяга МСП

☐ Няма ефект

11. Проектът на нормативен акт изисква ли цялостна оценка на въздействието?

☐ Да

☐ Не

12. Обществени консултации:

Обобщете най-важните въпроси за консултации в случай на извършване на цялостна оценка на въздействието или за обществените консултации по чл. 26 от Закона за нормативните актове. Посочете индикативен график за тяхното провеждане и видовете

Въпросите, посочени по-долу, са насочени към всички заинтересовани страни. Същите предстои да бъдат поставени на обсъждане в рамките на обществената консултация на проекта на Закон за изменение и допълнение на Закона за защита на личните данни по чл. 26 от Закона за нормативните актове.

Към всички заинтересовани страни:

1. Подходящо ли е въвеждането на диференциран режим за носене на административно-наказателна отговорност от страна на администраторите – публични органи и ако - да, защо?

2. Какви критерии са подходящи за постигане на баланс между правото на защита на личните данни, от една страна и правото на свобода на изразяване и информация, от друга, вкл. когато обработването на лични данни е за журналистически цели, достъп до обществена информация и др.?

3. За кои цели, съответно в кои специални закони, е необходимо и удачно да се въведат допълнителни условия по отношение на обработването на генетични данни, биометрични данни или данни за здравословното състояние?

4. В кои случаи е абсолютно необходимо да се обработва единният граждански номер/личният номер на чужденец и защо? В кои специални закони следва да се направят съответните промени?

5. Нужна ли е законодателна регламентация на видеонаблюдението за лични и домашни цели и ако - да, в кои негови аспекти?

6. В кои случаи извън задължителните по чл. 37 от Регламент 2016/679 е целесъобразно администраторите на лични данни да бъдат задължени да определят т.нар. длъжностно лице по защита на данните? Посочете мотиви за това.

7. Като се отчита наличната технология и разходите по изпълнението, какви биха били разумните стъпки и технически мерки от страна на администраторите на лични данни за практическото реализиране на:

- „правото да бъдеш забравен“?
- правото на преносимост на данните?

8. Какви средства биха били необходими за изпълнение на всички задължения на администраторите на лични данни, произтичащи от Регламент 2016/679 според следното разпределение на администраторите по категории:

- микропредприятия;
- малки предприятия;
- средни предприятия.

9. В обхвата на сертифицирането за защита на данните следва да бъдат включени едно или няколко от следните:

- услуги;
- продукти;
- системи;
- всички по-горе изброени.

10. Считате ли за целесъобразно КЗЛД да извършва сертифициране на длъжностните лица по защита на личните данни преди да им бъде възложено да изпълняват тези функции?

11. Кой модел за акредитация на сертифициращи органи считате за най-подходящ и защо:

- Акредитацията да се извършва единствено от КЗЛД;
- Акредитацията да се извършва единствено от Българската служба за акредитация;
- Акредитацията да се извършва от всеки от горните органи, независимо един от друг.

12. Следва ли да бъдат предприети законови мерки за насърчаване на администраторите на лични данни да прибягват до сертифициране и, ако да-какви?

13. Кой модел за сертифициране считате за най-подходящ и защо:

• Сертифицирането да се осъществява от организации, акредитирани специално за тази цел;

- Сертифицирането да се осъществява от КЗЛД.

14. Кой орган от долу изброените считате за най-подходящ да осъществява наблюдение на одобрен кодекс за поведение и защо:

- Съответният компетентен орган при отчитане на предмета на кодекса, акредитиран за

тази цел от КЗЛД;

- Комисията за защита на личните данни.

15. Следва ли да бъдат предвидени законови механизми, които да насърчават секторни кодекси за поведение и ако да, какви трябва да са те?

16. Виждате ли полза в използването на кодекси за поведение и какви кодекси считате за най-удачни – секторни кодекси или кодекси по конкретни форми на обработване на лични данни?

17. Следва ли КЗЛД (в ролята ѝ на надзорен орган) да предлага възможности за обучение в сферата на защитата на личните данни, с цел установяване на единни стандарти за работа с лични данни в България?

18. Следва ли да се търсят разнообразни форми за провеждане на обучение в сферата на защитата на личните данни, например онлайн обучение, дистанционно обучение и т.н.? Ако да, какви други форми на обучение считате за необходими?

19. Считате ли за целесъобразно КЗЛД да извършва задължително обучение на длъжностните лица по защита на личните данни преди да им бъде възложено да изпълняват тези функции?

20. Считате ли за целесъобразно задължителното обучение за длъжностните лица по защита на данните да бъде безплатно?

21. Считате ли за целесъобразно обучение в областта на защитата на личните данни, проведено от КЗЛД, различно от задължителното обучение, когато е по искане на администраторите, обработващите или обучаващите се, да бъде за тяхна сметка?

22. Какви законови стимули могат да бъдат предвидени за администраторите, за да бъдат мотивирани те да участват чрез свои представители в обучения, предлагани от КЗЛД?

23. В кои случаи извън посочените в чл. 37, пар. 1 от Регламент 2016/679 считате за подходящо задължително да бъде определяно длъжностно лице по защита на данните и защо?

24. Чл. 49, пар. 5 от Регламент 2016/679 допуска при липса на решение относно адекватно ниво на защита националното законодателство да определи (по важни причини от обществен интерес) ограничения за предаването на специални категории лични данни на трета държава или международна организация. Подкрепяте ли подобна възможност и ако – да, защо?

25. Разпоредбата на чл. 80, пар. 2 от Регламента допуска на национално ниво да бъде уредена възможност структури, организации и сдружения с нестопанска цел да имат право да подават жалба до надзорния орган по защита на данните, ако считат, че правата на субект на данни са нарушени, независимо дали субектът на данни е поискал това. Подкрепяте ли подобна възможност и ако – да, защо?

Към компетентните органи по директива 2016/680

1. При кои конкретни категории на обработване на лични данни считате, че е целесъобразно администраторът да забави, ограничи или да не предостави информация на субектите на данни (физическите лица, за които се отнасят данните)?

Към съдебните органи

1. Като се има предвид, че Регламент 2016/679 изрично освобождава съдилищата от надзора на Комисията за защита на личните данни, когато обработването на лични данни е при изпълнение на техните съдебни функции, кой е най-удачният модел за упражняване на вътрешен надзор върху обработване на лични данни от съдилищата в тези случаи?

Проектът на Закон за изменение и допълнение на Закона за защита на личните данни ще бъде публикуван на Портала за обществени консултации и на интернет страницата на МВР, в съответствие с чл. 26 от ЗНА.

Съгласно чл. 26, ал. 4 от Закона за нормативните актове срокът за предложения и становища по проектите, публикувани за обществени консултации е не по-кратък от 30 дни. При изключителни случаи, съставителят на проекта може да определи друг срок, но не по-кратък от 14 дни. Предвид обстоятелството, че срокът за транспониране в българското законодателство на Директива 2016/680/ЕС е 6 май 2018 г., срокът за обществено обсъждане на портала за обществени консултации и на интернет страниците на МВР е намален на 14 дни.

Проектът на Закон за изменение и допълнение на Закона за защита на личните данни ще се съгласува в съответствие с чл. 32, ал. 1 от Устройствения правилник на Министерския съвет и

на неговата администрация.

13. Приемането на нормативния акт произтича ли от правото на Европейския съюз?

✓ Да
Не

Задължението за предприемане на нормативната промяна произтича от чл. 63, пар. 1 от Директива 2016/680. В допълнение, долу изброените разпоредби на Регламент 2016/679 също изискват задължително приемане на законови мерки на национално ниво или налагат държавите-членки да уредят законодателно по избор определени възможности:

- Чл. 43, пар. 1;
- Чл. 51, пар. 4;
- Чл. 84;
- Чл. 85, пар. 1 и пар. 2;
- Чл. 8, пар. 1;
- Чл. 36, пар. 5;
- Чл. 37, пар. 4;
- Чл. 80, пар. 2;
- Чл. 23;
- Чл. 89, пар. 2 и пар. 3;
- Чл. 6, пар. 2 и пар. 3;
- Чл. 9, пар. 4;
- Чл. 87;
- Чл. 88;
- Чл. 90.

Информация по отношение т. 8.1 от настоящия документ – с чл. 84, пар. 1 от Регламент 2016/679 се отменя Директива 95/46/ЕО, въз основа на която е въведен режим на регистрация на администраторите на лични данни. Във връзка с това се отменят текстовете от ЗЗЛД, уреждащи режима на регистрация.

Информация по отношение т. 8.2 от настоящия документ:

Двата нови режима на акредитиране и сертифициране произтичат от чл. 42 и чл. 43 от Регламент 2016/679.

Двата съществуващи режима, които се засягат и правното основание, от което произтича това, са:

-отпадането на регистрацията на администратори - в резултат от отмяната на Директива 95/46/ЕО по аргументи, посочени по-горе (чл. 84, пар. 1 от Регламент 2016/679);

- облекчаване на режима на трансфери на данни – в резултат на подробната правна уредба на този въпрос в Глава V от Регламент 2016/679.

Моля посочете изискванията на правото на Европейския съюз, включително информацията по т. 8.1 и 8.2, дали е извършена оценка на въздействието на ниво Европейски съюз, и я приложете (или посочете връзка към източник).

14. Име, длъжност, дата и подпис на директора на дирекцията, отговорна за изработването на нормативния акт:

Име и длъжност: Снежина Маринова, директор на дирекция „ЕС и международно сътрудничество“ – МВР

Дата: 30.03.2018 г.

Подпис:

Маринова