

Правен бюлетин

Акценти в броя:

Обнародвани нормативни актове

- Закон за изменение и допълнение на Закона за електронното управление
- Закон за изменение и допълнение на Закона за вътрешния одит в публичния сектор
- Наредба № Н-2 от 30 юни 2016 г. за реда и начина за осъществяване, координация и хармонизация на специфичните одитни дейности по фондове и програми на Европейския съюз

Внесени законопроекти

- Законопроект за противодействие на тероризма
- Закон за изменение на Кодекса на труда
- Закон за изменение и допълнение на Закона за защита от дискриминация

Анализи

МИС Директивата – крачка в правилната посока в областта на киберсигурността



Обнародвани нормативни актове

Закон за изменение и допълнение на Закона за електронното управление (ДВ бр. 50 / 01.07.2016 г.)

Основната цел на измененията е създаването на инфраструктура за управление на дейностите в областта на електронното управление. Създава се Държавна агенция „Електронно управление“ към Министерския съвет. Агенцията осъществява сътрудничество и взаимодействие по въпросите на електронното управление с компетентните органи на държавите – членки на ЕС, с институциите на ЕС и с други международни организации.

Образува се държавно предприятие „Единен системен оператор“. Предприятието подпомага председателя на ДА „Електронно управление“, като:

- информационен контактен център за обслужване на гражданите и бизнеса в областта на електронното управление;

- помощен контактен център за обслужване на държавните органи, използващи споделените информационни ресурси на електронното управление;
- национален център за действие при инциденти относно информационната сигурност;
- изгражда и поддържа Национален портал за пространствени данни, чрез който се осъществява връзката с геопортала на инфраструктурата за пространствена информация на Европейската общност (INSPIRE).

Предприятието следва също да подпомага администрациите при осъществяване на функциите им посредством следните вътрешни услуги:

- непрекъснат мониторинг, регистриране на инциденти, диагностициране на проблеми и управление на поддръжката на споделените

информационни ресурси на електронното управление;

- регистриране на инциденти, диагностициране на проблеми, управление на поддръжката и контрол на промените на системния и приложния софтуер, информационните системи и електронните услуги, разположени върху споделените информационни ресурси на електронното управление;
- управление на капацитета и разпределението на ресурсите между всички държавни органи, използващи споделените информационни ресурси на електронното управление;
- първоначално конфигуриране и въвеждане на нови услуги върху споделените информационни ресурси на електронното управление;
- изграждане, развитие и поддръжка на среда за тестване на електронни административни услуги върху споделените информационни ресурси на електронното управление;
- контрол на изпълнението на договори по развитие и поддръжка на споделените информационни ресурси на електронното управление;
- извършване на специализирани одити и анализи в областта на електронното управление, информационните и комуникационните технологии, както и на мрежовата и информационната сигурност;
- консултации и разработване на проекти на системни и приложни архитектури за информационни системи и електронни услуги;
- изготвяне на технически спецификации по програми, проекти и поръчки на всички административни органи в областта на електронното управление, информационните и комуникационните технологии при стойност за възлагане на обществена поръчка за доставки и услуги над праговете по чл. 20, ал. 1, т. 1, буква „б“ и ал. 2, т. 2 от Закона за обществените поръчки;
- управление на изпълнението на проекти за електронно управление, информационни и комуникационни технологии;
- контрол и участие при приемане на изпълнението на работата на изпълнители по договори за възлагане на обществени поръчки за доставки и услуги в областта на електронното управление, информационните и комуникационните технологии;

- управление и контрол на оперативната съвместимост и подпомагане на процеси и осъществяване на дейности по интеграция на информационни системи и електронни административни услуги.

Освен гореизброените функции, предприятието осъществява следния предмет на дейност само на територията на България:

- предоставяне на услуги в областта на електронното управление и информационните и комуникационните технологии;
- предоставяне на услуги по анализ на бизнес и технологични процеси, управление на проекти и контрол на качеството;
- предоставяне на услуги в областта на оперативната съвместимост;
- предоставяне на услуги в областта на мрежовата и информационната сигурност;
- извършване на други дейности, които осигуряват или допълват основния предмет на дейност.

Закон за изменение и допълнение на Закона за вътрешния одит в публичния сектор (ДВ бр. 51 / 05.07.2016 г.)

Промените налагат задължението вътрешният одит да се осъществява в съответствие с международните стандарти за професионална практика по вътрешен одит. Въвеждат се редица промени в регламентацията на звената за вътрешен одит и одитните комитети. Изменят се и правата и задълженията на вътрешните одитори.

Наредба № Н-2 от 30 юни 2016 г. за реда и начина за осъществяване, координация и хармонизация на специфичните одитни дейности по фондове и програми на Европейския съюз (ДВ бр. 52 / 08.07.2016 г.)

Съгласно наредбата, специфичните одитни дейности по фондове и програми на ЕС включват:

- одити на системите за оценка на правилното функциониране на системите за управление и контрол на съответната оперативна програма;
- одити на операциите за оценка на законосъобразността и редовността на декларираните пред Европейската комисия разходи;

- одити на отчетите за оценка на пълнотата, точността и верността на сумите, декларирани в годишните счетоводни отчети;
- издаване на годишни контролни доклади, годишни становища и декларации за приключване на програмите, съфинансирани от фондове на Европейския съюз, които обобщават резултатите от изпълнените одитни дейности по горните точки.

Специфичните одитни дейности следва да се извършват от Изпълнителна агенция „Одит на средствата от Европейския съюз“ към министъра на финансите.

Други обнародвани нормативни актове:

Закон за изменение и допълнение на Закона за подпомагане и финансова компенсация на пострадали от престъпления (ДВ бр. 51 / 05.07.2016 г.)

Закон за изменение и допълнение на Закона за защита при бедствия (ДВ бр. 51 / 05.07.2016 г.)

Закон за ратифициране на Споразумение за създаване на регионален доверителен фонд на Европейския съюз в отговор на сирийската криза, „Фонд Мадад“, и неговите вътрешни правила между Генералната дирекция за сътрудничество за развитие на Италианското министерство на външните работи и международното сътрудничество и Европейската комисия от името на Европейския съюз и на Сертификат за принос на донорите, част от Приложение II от Споразумението за създаване на регионален доверителен фонд на Европейския съюз в отговор на сирийската криза, „Фонд Мадад“, и неговите вътрешни правила между Генералната дирекция за сътрудничество за развитие на Италианското министерство на външните работи и международното сътрудничество и Европейската комисия от името на Европейския съюз (ДВ бр. 51 / 05.07.2016 г.)

Закон за изменение и допълнение на Закона за водите (ДВ бр. 52 / 08.07.2016 г.)

Закон за изменение и допълнение на Закона за културното наследство (ДВ бр. 52 / 08.07.2016 г.)

Закон за ратифициране на Протокола към Северноатлантическия договор относно присъединяването на Черна гора (ДВ бр. 52 / 08.07.2016 г.)

Закон за изменение и допълнение на Закона за сдружения за напояване (ДВ бр. 54 / 15.07.2016 г.)

Постановление № 153 от 24 юни 2016 г. за изменение и допълнение на Правилника за прилагане на Закона за

регионалното развитие, приет с Постановление № 216 на Министерския съвет от 2008 г. (ДВ бр. 50 / 01.07.2016 г.)

Постановление № 154 от 28 юни 2016 г. за изменение на Постановление № 181 на Министерския съвет от 2009 г. за определяне на стратегическите обекти и дейности, които са от значение за националната сигурност (ДВ бр. 51 / 05.07.2016 г.)

Постановление № 157 от 30 юни 2016 г. за одобряване на допълнителни трансфери по бюджетите на общините за 2016 г. за финансово осигуряване на дейностите по Модул „Оптимизиране на вътрешната структура на училищата, детските градини и самостоятелните обществени“ от Национална програма „Оптимизация на училищната мрежа“, одобрена с Решение № 271 на Министерския съвет от 2016 г. за одобряване на национални програми за развитие на средното образование (ДВ бр. 51 / 05.07.2016 г.)

Постановление № 160 от 1 юли 2016 г. за определяне правилата за разглеждане и оценяване на оферти и сключването на договорите в процедурата за избор с публична покана от бенефициенти на безвъзмездна финансова помощ от Европейските структурни и инвестиционни фондове (ДВ бр. 52 / 08.07.2016 г.)

Постановление № 161 от 4 юли 2016 г. за определяне на правила за координация между управляващите органи на програмите и местните инициативни групи, и местните инициативни рибарски групи във връзка с изпълнението на Подхода „Водено от общностите местно развитие“ за периода 2014 – 2020 г. (ДВ бр. 52 / 08.07.2016 г.)

Постановление № 162 от 5 юли 2016 г. за определяне на детайлни правила за предоставяне на безвъзмездна финансова помощ по програмите, финансирани от Европейските структурни и инвестиционни фондове за периода 2014 – 2020 г. (ДВ бр. 53 / 12.07.2016 г.)

Постановление № 167 от 8 юли 2016 г. за определяне на реда за предоставяне на безвъзмездна финансова помощ по фонд „Убежище, миграция и интеграция“ и фонд „Вътрешна сигурност“ за периода 2014 – 2020 г. (ДВ бр. 54 / 15.07.2016 г.)

Постановление № 168 от 8 юли 2016 г. за изменение и допълнение на Наредбата за пенсиите и осигурителния стаж, приета с Постановление № 30 на Министерския съвет от 2000 г. (ДВ бр. 54 / 15.07.2016 г.)

Наредба за изменение и допълнение на Наредба № 9 от 2000 г. за условията и реда за провеждане на конкурси за възлагане на управлението на лечебни

заведения по Закона за лечебните заведения (ДВ бр. 50 / 01.07.2016 г.)

Наредба за изменение и допълнение на Наредба № 3 от 2015 г. за условията и реда за прилагане на схемите за директни плащания (ДВ бр. 50 / 01.07.2016 г.)

Наредба за допълнение на Наредба № Н-12 от 2014 г. за условията и реда за предоставяне на финансова или материална помощ и за предоставяне на помещения във военните клубове или в сгради в управление на Министерството на отбраната или структурите на пряко подчинение на министъра на отбраната (ДВ бр. 50 / 01.07.2016 г.)

Наредба за изменение и допълнение на Наредба № 11 от 2007 г. за условията и реда за признаване на организации на производители на плодове и зеленчуци и на техните асоциации и за условията и реда за одобряване и изменение на одобрените оперативни програми (ДВ бр. 52 / 08.07.2016 г.)

Наредба за изменение и допълнение на Наредба № 7 от 2001 г. за реда за посещение, маневриране и престой на корабите в пристанищата и рейдовете, за товарене и разтоварване, за качване на кораба и слизане на брега на екипажа, на пътниците или други лица, както и за връзка на кораба с брега (ДВ бр. 52 / 08.07.2016 г.)

Наредба за изменение и допълнение на Наредба № 1 от 2016 г. за прилагане на подмярка 19.4. „Текущи разходи и популяризиране на стратегия за Водено от общностите местно развитие“ на мярка 19. „Водено от общностите местно развитие“ от Програмата за развитие на селските райони за периода 2014 – 2020 г. (ДВ бр. 53 / 12.07.2016 г.)

Наредба за изменение и допълнение на Наредба № 27 от 2014 г. за статистиката на платежния баланс, международната инвестиционна позиция и статистиката на ценните книжа (ДВ бр. 53 / 12.07.2016 г.)

Конвенция за взаимно административно сътрудничество по данъчни въпроси, изменена с Протокола за изменение на Конвенцията за взаимно административно сътрудничество по данъчни въпроси, влязъл в сила на 1 юни 2011 г. (ДВ бр. 50 / 01.07.2016 г.)

Многостранно споразумение между компетентните органи за автоматичен обмен на информация за финансови сметки (ДВ бр. 50 / 01.07.2016 г.)

Споразумение между Агенцията за ядрено регулиране на Република България (АЯР) и Националната комисия за контрол на ядрените дейности (НККЯД) на Румъния за обмен на техническа информация и сътрудничество

при регулирането и контрола на ядрената безопасност и радиационната защита (ДВ бр. 50 / 01.07.2016 г.)

Гаранционно споразумение между Банката за развитие на Съвета на Европа в качеството на бенефициент и Република България в качеството на гарант (ДВ бр. 51 / 05.07.2016 г.)

Внесени законопроекти

Законопроект за противодействие на тероризма (внесен от Министерски съвет на 07.07.2016 г.)

Основните цели на предложения закон са:

- (i) защита на правата на гражданите, юридическите лица, държавата и обществото от тероризъм;
- (ii) превенция чрез установяване и отстраняване на причините и условията, способстващи извършването на тероризъм;
- (iii) разработване на механизъм и индикатори за идентифициране, наблюдение и оценка на рисковете и предотвратяване на вредните последици от тероризъм.

Закон за изменение на Кодекса на труда (внесен от народни представители на 08.07.2016 г.)

Предложеният законопроект е насочен към намаляване на тежестта на административната процедура за сключване, регистриране и отчитане на едnodневни трудови договори по чл. 114а, ал. 1 от КТ.

Закон за изменение и допълнение на Закона за защита от дискриминация (внесен от Министерски съвет на 08.07.2016 г.)

Законопроектът има за цел да приведе чл. 4, ал. 3 и § 1, т. 7 от Закона за защита от дискриминацията в съответствие с Директива 2000/43/ЕО на Съвета от 29 юни 2000 година относно прилагане на принципа на равно третиране на лица без разлика на расата или етническия произход. Разпоредбите дефинират концепциите за „непряка дискриминация“ и „неблагоприятно третиране“.

Анализи

Директива за мрежова и информационна сигурност (МИС) – крачка в правилната посока в областта на киберсигурността

„Всяка програма за действие носи своя риск и цена – но те бледнеят пред дългосрочната цена на

удобното бездействие.“ – този неостаряващ призив на американския президент Джон Ф. Кенеди е подобаваща оценка на начина, по който развитите икономики се справят със светкавичното развитие на технологиите и растящата заплаха за киберсигурността, която неминуемо го следва. Изминалата 2015-та година е особено показателна за последиците от институционалното бездействие. По данни на Identity Theft Resource Center в рамките на годината кибератаки са довели до 781 разгласени системни пробиви в редица ключови сектори, сред които финансовия, образователния, държавния и здравния. В резултат от тези пробиви над 169 милиона лични досиета са станали уязвими. На глобално ниво, средната цена на откраднатото досие, съдържащо конфиденциална информация, е била \$ 154. На фона на тези показатели, едва 38% от компаниите и държавните организации твърдят, че имат готовност да се справят със софистицирана кибератака.

В отговор на растящите заплахи за киберсигурността на Европейския съюз, на 06.07.2016 г. Европейският парламент прие Директива на Европейския парламент и на Съвета относно мерки за гарантиране на високо общо ниво на мрежова и информационна сигурност на Съюза (наричана по-долу „МИС Директивата“ или „Директивата“). Директивата, която представлява основна част от европейската стратегия за киберсигурност, влиза в сила през август 2016 г., като държавите-членки ще имат 21 месеца да я транспонират в местното си законодателство.

Несъмнен е фактът, че Директивата ще има дълбоко въздействие върху публичния и частния сектор в България. Транспонирането ѝ ще доведе до изграждането на нови структури в изпълнителната власт, както и до допълнителни задължения за частния бизнес. Настоящият текст има за цел да предложи цялостен анализ на МИС Директивата и нейното въздействие, както и да я постави в контекста на европейските мерки в областта на киберсигурността.

Европейският съюз и киберсигурността – сложни взаимоотношения

Първите стъпки в областта на киберсигурността на европейско ниво почват още през 2001 г. Тогава Европейската комисия (ЕК) издава „Мрежова и информационна сигурност: предложение за създаване на европейска политика“, в което се подчертава растящата значимост на мрежовата и информационната сигурност. Предложението е последвано от приемането на Стратегия за сигурно информационно общество през

2006 г., което има за цел да развие култура на мрежова и информационна сигурност в рамките на Европейския съюз. В последвалите години Съобщението относно защитата на критичната информационна инфраструктура и Програмата в областта на цифровите технологии за Европа, приети през 2009 г., поставят допълнителен акцент върху важната роля на мрежовата и информационната сигурност.

Въпреки изразената готовност за изграждане на мерки за противодействие на кибератаки, малка част от добрите намерения на европейските законодатели се превръщат в нормативни актове. Основното постижение в сферата е изграждането на изцяло нова инфраструктура за мрежова и информационна сигурност. През 2004 г., посредством Регламент (ЕО) № 460/2004, се създава Европейската агенция за мрежова и информационна сигурност, а 8 години по-късно ЕК приема съобщение относно създаването на Европейски център по киберсигурност, част от Европейската полицейска служба.

Успоредно с това се приемат регулаторна рамка за защита на данните и ревизирана регулаторна рамка за електронните съобщения, които налагат въвеждането на определени мерки за сигурност. С Директива 2008/114/ЕО се създава Европейската програма за защита на критичната инфраструктура, която определя общия подход към защитата на критичните инфраструктури на ЕС.

МИС Директивата

Въпреки направените стъпки в правилната посока, ЕС остава далеч от адекватна система за противодействие на кибератаки. Това виждане се споделя и от частния сектор, както е видно от обществената консултация на тема „Подобряване на МИС в ЕС“, проведена от ЕК. Основните притеснения, изразени в консултацията, са необходимостта да се прави повече за мрежовата и информационната сигурност на национално ниво, както и липсата на европейско законодателство в областта на киберсигурността.

В отговор на тези притеснения и на зачествящите кибератаки, Европейската комисия прие МИС Директивата. На първо място с нея се налагат редица мерки на национално ниво. Държавите-членки се задължават да приемат национална стратегия за мрежова и информационна сигурност, с която следва да се определят стратегически цели, конкретни политически и регулаторни мерки за постигане и поддържане на високо равнище на мрежова и

информационна сигурност. Националната стратегия съдържа също и национален план за сътрудничество за мрежова и информационна сигурност, който да определя процесите на сътрудничество и комуникация, ролите и отговорностите на различните действащи лица, участващи в изпълнението на плана, и други.

В допълнение към националната стратегия, всяка държава-членка следва да сформира национални компетентни органи по сигурността на мрежовите и информационните системи. Компетентните органи на държавите-членки и ЕК следва да формират мрежа на сътрудничество срещу рискове и инциденти, засягащи мрежовите и информационните системи. Основните цели на мрежата за сътрудничество са постигане на навременна реакция при сериозни заплахи пред киберсигурността на ЕС и развиването на най-добри практики в сферата на киберсигурността, както на европейско, така и на национално ниво. За целта е предвидено изграждането на необходимата инфраструктура за обмен на конфиденциална информация, а на ЕК са поверени правомощията да приема План на Съюза за сътрудничество за МИС.

Основен метод за постигане на навременна реакция при киберзаплахи са така наречените „ранни предупреждения“. Директивата налага задължение на компетентните органи на държавите-членки да отправят ранни предупреждения в мрежата за сътрудничество по отношение на рискове и инциденти, които отговарят на поне един от следните критерии:

- (i) мащабът им се увеличава бързо или може да се увеличи бързо;
- (ii) превишават или може да превишат националния капацитет за отговор;
- (iv) засягат или може да засегнат повече от една държава членка.

Така регламентирани, ранните предупреждения дават предпоставката за високо ниво на организираност в рамките на целия съюз, необходимо за справяне с по-сериозните заплахи пред мрежовите и информационните системи. Въпреки това, всяка предварителна оценка на системата е форма на гадаене, тъй като функционалността и адекватността ѝ се крепят основно на капацитета и способността на отделните компетентни органи на държавите-членки да се справят с предизвикателствата, които възникват. От своя страна, тези фактори до голяма степен зависят от политическата и икономическа обстановка в съответната държава-членка.

В следващата си част, Директивата налага на публичната администрация и пазарните оператори задължението да „предприемат подходящи технологически и организационни мерки за управление на рисковете, пред които е изправена сигурността на мрежите и информационните системи, които контролират и използват като част от дейността си.“ Предприетите мерки следва да гарантират ниво на сигурност, което съответства на съществуващия риск, като се имат предвид последните постижения в съответната сфера.

Предвижда се още задължение за публичната администрация и пазарните оператори да докладват на компетентния орган на съответната държава-членка при инциденти, които имат значим ефект върху сигурността на основните услуги, които предлагат.

Изискванията важат за всички пазарни оператори, предоставящи услуги на територията на ЕС, като терминът включва:

- (i) доставчици на услуги на информационното общество, които правят възможно предоставянето на други услуги на информационното общество (напр. социални мрежи, облачни услуги, платформи за електронна търговия и др.);
- (ii) оператори на критична инфраструктура, която е от основно значение за поддържането на особено важни икономически и обществени дейности в сферата на енергетиката, транспорта, банковото дело, фондовите борси и здравеопазването (напр. доставчиците на газ, кредитни институции, летища и др.).

Изискванията няма да се прилагат за микропредприятия, както са дефинирани в Препоръка 2003/361/ЕО на Комисията от 6 май 2003 г. относно определението за микро-, малки и средни предприятия.

Директивата предвижда също и мерки за прилагане на гореописаните задължения, като компетентните органи следва да могат да изискват от пазарните оператори и публичните администрации предоставянето на информация, необходима за оценка на сигурността на техните мрежи и информационни системи, както и да се подложат на одит на сигурността, извършен от квалифицирана независима организация или национален орган. Компетентните органи ще имат също и възможността да издават задължителни инструкции за участниците на пазара и публичните администрации. Предвиден е механизъм за оспорване на задълженията, наложени от компетентните органи.

Изискванията, които Директивата въвежда, означават, че голяма част от ключовите оператори в частния сектор ще бъдат задължени да въведат най-модерните системи за управление на риска, като цената на тази стъпка все още не е ясна. Проведената от Комисията обществена консултация на тема „Подобряване на МИС в ЕС“ сочи, че за голяма част от участниците в консултацията (63.4%) това няма да представлява значително финансово бреме. Подобни са настроенятия и по отношение на разходите във връзка с докладването на инциденти (мнозинство от 72.3%). Въпреки това, все още е трудно да се каже дали и доколко новите изисквания ще представляват особена финансова тежест за българските предприятия.

В допълнение на гореописаните финансови притеснения, Директивата създава предпоставки и за административно обременяване на дружествата.

При некомпетентно или недобросъвестно прилагане, правомощията на националните компетентни органи да изискват определени действия от страна на пазарните оператори могат да създадат сериозни административни пречки пред нормалните работни процеси в частния сектор. Така например възможността да се изисква предоставянето на информация, необходима за оценка на сигурността на мрежи и информационни системи, е разписана без никаква конкретика относно типа документи, за който се отнася. Широко тълкуване на тази разпоредба от страна на съответния национален компетентен орган би могло да доведе до административен произвол, под претекста, че се събира необходима информация, с което сериозно да се наруши работния процес в съответния пазарен оператор. Доколко проблеми от този тип могат да станат реалност в България, предстои да видим в следващите няколко години.

Пътят напред

Новоприетата Директива представлява явна индикация за намеренията на Европейския съюз да създаде правна рамка, която да може адекватно да противодейства на заплахите за киберсигурността за частния и публичния сектор. За пръв път в ЕС – в лицето на националните компетентни органи – ще заработи инфраструктура, която има необходимия капацитет и обхват за постигане на тези цели. В допълнение се налагат редица задължения за частния и публичния сектор, които да осигурят своевременно засичане на заплахи и бърза реакция, както на национално, така и на общностно ниво. Новите разпоредби неминуемо водят със себе си притеснения за пречките, които могат да се създадат за развитието

на частния бизнес. Доколко тези притеснения са основателни, обаче, предстои да видим в следващите години. За момента можем да се радваме, че погледът на ЕС е насочен в правилната посока.



Христо Милушев
Адвокатски сътрудник

За контакти

адв. Ренета Петкова
Съдружник
rpetkova@deloittece.com

адв. Звезделина Филова
Мениджър
zfilova@deloittece.com

Адвокатско дружество
„Делойт Лигъл“
бул. „Ал.Стамболийски“ 103
София Тауър (Мол София)
гр. София 1303
България
Телефон: + 359 (2) 8023 300
Факс: + 359 (2) 8023 350
www.deloitte.bg