Приложение № 3 към чл. 17

видове защити / нива на защита	физическа		персонална	документална	автоматизирани информационни системи и/или мрежи		криптографска
	организационни мерки	технически мерки	организационни мерки	организационни мерки	организационни мерки	технически мерки	технически мерки
ниско	* определяне на помещенията, в които ще се обработват лични данни; * определяне на **помещенията**, **в които ще се** разполагат елементите на комуникационно-информационните системи за обработване на лични данни; * определяне на организацията на физическия достъп;	*ключалки; * шкафове; * пожарогасителни средства; * оборудване на **помещенията**;	* познаване на нормативната уредба в областта на защитата на личните данни; * знания за опасностите за **личните данни**, **обработвани** от администратора; * съгласие за поемане на задължение за неразпространение на личните данни;	* определяне на регистрите, които ще се поддържат на хартиен носител; * определяне на условията за **обработване на лични данни**; * регламентиране на достъпа до регистрите; * определяне на срокове за съхранение; * процедури за унищожаване;	* персонална защита; * определяне на срокове за съхранение на личните данни; * процедури за **унищожаване/заличаване/изтр**иване на носители;	* идентификация и автентификация; * управление на регистрите; * външни връзки/свързване; * **защита от вируси**; * копия/резервни копия за възстановяване; * носители на информация;	
средно	* **ниско ниво +** * определяне на използваните технически средства за физическа защита; * определяне на зоните с контролиран достъп;	* **ниско ниво**	* **ниско ниво +** * обучение; * споделяне на критична информация между персонала; * познаване на политиката и ръководствата за защита на личните данни; * тренировка на персонала за реакция при събития, застрашаващи сигурността на данните;	* **ниско ниво +** * контрол на достъпа до регистрите; * правила за размножаване и разпространение;	* **ниско ниво +** * физическа среда/ обкръжение;	* **ниско ниво +** * телекомуникации и отдалечен достъп; * поддържане/ експлоатация;	* стандартните криптографски възможности на операционните системи; * стандартните криптографски възможности на системите за управление на бази данни; *стандартните криптографски възможности на комуникационното оборудване;
високо	* **средно ниво +** * определяне на екип за реагиране при нарушения; * определяне на режима на посещения;	* **средно ниво +** * пожароизвестителни и пожароизвестителни системи; * оборудване на зоните с контролиран достъп; * охрана и/или система за сигурност; * устройства за контрол на физическия достъп; * детектори за субстанции; * средства за защита на периметъра;	* **средно ниво**	* **средно ниво +** * процедури за проверка и контрол на обработването;	* **средно ниво +** * политики за защита на личните данни, ръководства по защита и стандартни операционни процедури; * планиране на случайността/непредвидените случаи; * тренировка на персонала за реакция при събития, застрашаващи сигурността на данните;	* **средно ниво +** * определяне на роли и отговорности; * контроли на сесията; * наблюдение; * управление на конфигурацията;	* **средно ниво +** * нормативно определените системи за електронен подпис; *системи за разпределение и управление на криптографските ключове;
изключително високо	* **високо ниво +** * мерки, произтичащи от международни политики за сигурност или актове с международен характер.						