Основно училище "Георги Бенковски"
с. Галата, ул." Никола Вапцаров" № 1, 069031/0893328106,ou_galata@abv.bg

Приложение I
Към чл. 5, т. 6 Технически и организационни мерки за защита на личните данни

1. ОБРАБОТВАЩИЯТ третира всички лични данни, предадени от АДМИНИСТРАТОРА или възникнали по време на обработката, като поверителни, като не ги разкрива, освен на служителите си и обработващи подизпълнители и само до колкото това е необходимо за изпълнение на дейностите по договора.

2. ОБРАБОТВАЩИЯТ поддържа политики, инструкции или насоки, които преразглежда и обновява, ако е необходимо, най-малко веднъж годишно, регулиращи сигурността на информацията и в частност на защитата на личните данни, а както и ИТ сигурността.

3. ОБРАБОТВАЩИЯТ гарантира, че служителите му:

3.1. са се задължили писмено да спазват поверителността на личните данни;

3.2. познават съответните му политики, инструкции и насоки във връзка със защита на личните данни;

3.3. познават законодателството за защита на данните;

3.4. знаят какви мерки и действия да предприемат при евентуален пробив в сигурността на личните данни;

3.5. са квалифицирани да изпълняват възложените им задачи във връзка с обработката на личните данни.

4. ОБРАБОТВАЩИЯТ поддържа необходимото ниво на контрол върху помещенията, в които се обработват данните, включително сървърни или сходни помещения, което да предотврати неоторизиран достъп до тях.

5. ОБРАБОТВАЩИЯТ взима необходимите мерки за допълнителни физически ограничения пред нерегламентирания и/или неоторизиран достъп до лични данни (ключалки, шкафове, метални каси, оборудвани зони с контролиран достъп, оборудвани помещения, система за физически контрол на достъпа (вкл. бариери, камери за наблюдение), охранители и система за управление на сигурността, автоматична пожароизвестяване, аларма и пожарогасителна система, системи за защита на периметъра).

6. ОБРАБОТВАЩИЯТ поддържа регистър/логове на достъпите до помещенията, в които се обработват лични данни.

7. ОБРАБОТВАЩИЯТ поддържа възможността да се проследи всяко въвеждане, достъпване, модифициране, изтриване на лични данни от съответния служител.

8. ОБРАБОТВАЩИЯТ прилага специфични мерки за защита на автоматизираните системи, които използва както следва:

8.1. достъпът до системите е защитен и сигурен и се осъществява посредством удостоверяване;

8.2. правата на АДМИНИСТРАТОРИТЕ са ограничени до необходимостта от оперативно обслужване;

8.3. активно проверява актуалността на и актуализира предоставените достъпи и права до системите;

8.4. използва стандартните криптографски възможности на операционните системи, базите данни и комуникационното оборудване;

8.5. поддържа резервни копия и да може да възстанови загубени данни;

8.6. използва само лицензиран софтуер, който се обновява редовно особено по отношение на критичните обновявания;

8.7. използва актуална антивирусна защита;

8.8. максимално ограничава и контролира използването на Интернет от работните места, на които се извършва обработката;

8.9. прехвърля/събира данните само през сигурни протоколи TLS, HTTPS, SFTP и FTPS;

8.10. поддържа техническите мерки, които налагат затваряне на неактивни сесии, блокиране на акаунти след няколко последователни неуспешни опита за вход, силна парола или удостоверяване чрез парола и мерки, изискващи сигурен трансфер и съхранение на такива пароли;

8.11. избягва обработването на устройства, които не е сертифицирал и/или обслужил, ако това се налага проверява и настройва всяко едно такова устройство;

8.12. взима необходимите мерки за правилното изтриване и унищожаване на информацията от съответните носители.

9. ОБРАБОТВАЩИЯТ избягва съхраняването на лични данни върху преносими носители. Ако това неизбежно се налага, то същите следва да бъдат криптирани.

10. ОБРАБОТВАЩИЯТ документира, анализира и съобщава на АДМИНИСТРАТОРА за всички пробиви в сигурността, независимо дали се касае за физически документи или автоматизирани системи.

11. В случай на разработка на софтуер от страна на ОБРАБОТВАЩИЯ, за АДМИНИСТРАТОРА или от страна на трета страна за ОБРАБОТВАЩИЯ свързан с обработването на личните данни, последните не могат да бъдат използвани за тестване преди да бъдат анонимизирани или маскирани, така че да не позволяват идентифициране на данни за физически лица.

---

[1] Същите могат да бъдат адаптирани за всеки конкретен случай

[2] Трябва да се прецизира за всеки случай.