СРЕДНО УЧИЛИЩЕ „ ВАСИЛ КЪНЧОВ „ – ГРАД ВРАЦА
Ул. „ Хан Аспарух „ № 17, тел. / факс: 092 / 620361

УТВЪРЖДАВАМ:

ДИМИТЪР МАРКОВ

Директор на СУ „Васил Кънчов“-Враца

И Н С Т Р У К Ц И Я

ОТНОСНО ПРАВИЛА ЗА СИГУРНОСТ

ПРИ ОБРАБОТВАНЕТО НА ЛИЧНИ ДАННИ

В СРЕДНО УЧИЛИЩЕ „ВАСИЛ КЪНЧОВ“-ВРАЦА

I. Общи положения

Личните данни се събират за конкретни, точно определени от закона цели, обработват се законосъобразно и добросъвестно и не могат да се обработват допълнително по начин, несъвместим с тези цели. Достъп на лица до лични данни се предоставя единствено, ако те имат право на такъв достъп, съгласно действащото законодателство и след тяхното легитимиране. Информацията може да бъде предоставена под формата на:

1. устна справка;
2. писмена справка;
3. преглед на данните от самото лице;
4. предоставяне на исканата информация на технически и/или електронен носител.

II. Съхранение на личните данни

Личните данни се съхраняват на хартиен, технически и/или електронен носител, само за времето, необходимо за изпълнение на правни задължения на УЧЕБНОТО ЗАВЕДЕНИЕ и/или нормалното му функциониране.

Право на достъп до регистрите с лични данни имат само оторизираните длъжностни лица.Оторизирането се извършва на база длъжностна характеристика и/или чрез изрична заповед на Директора на УЧЕБНОТО ЗАВЕДЕНИЕ.

Служителите носят отговорност за осигуряване и гарантиране на регламентиран достъп до служебните помещения и опазване на регистрите, съдържащи лични данни. Всяко умишлено нарушение на правилата и ограниченията за достъп до личните данни от персонала може да бъде основание за налагане на дисциплинарни санкции.

Длъжностните лица нямат право да разпространяват информация за личните данни, станали им известни при изпълнение на служебните им задължения.

Документите и преписките, по които работата е приключила, се архивират.

Трайното съхраняване на документи, съдържащи лични данни, се извършва на хартиен носител в помещението, определено за архив, за срокове, съобразени с действащото законодателство. Помещението, определено за архив, е оборудвано с пожарогасител и задължително се заключва.

Съхранението на документите и преписките на хартиен носител, архивирането/унищожаването на тези с изтекъл срок, се извършва по реда на Закона за Националния архивен фонд.

Документите на електронен носител се съхраняват на специализирани компютърни системи.

Достъп до архивираните документи, съдържащи лични данни, имат единствено оторизирани лица.

С оглед защита на хартиените, техническите и информационните ресурси всички служители са длъжни да спазват правилата за противопожарна безопасност.

III. Унищожаване на регистри с лични данни

След постигане целта на обработване на личните данни или преди прехвърлянето на контрола върху обработването личните данни, съдържащи се в поддържаните от УЧЕБНОТО ЗАВЕДЕНИЕ регистри, следва да бъдат унищожени или прехвърлени на друг администратор на лични данни.

Личните данни, съхранявани на електронен носител, се унищожават чрез трайно изтриване, вкл. презаписването на електронните средства или физическо унищожаване на носителите. Документите на хартиен носител, съдържащи данни, се унищожават чрез нарязване.

Унищожаване се осъществява от служителя, отговорен за архива на УЧЕБНОТО ЗАВЕДЕНИЕ.

IV. Мерки по осигуряване на защита на личните данни

Като помещения, в които ще се обработват лични данни, се определят всички помещения, в които с оглед нормалното протичане на учебния и административния процес, се събират, обработват и съхраняват лични данни. Достъпът до тях е физически ограничен само за служители с оглед изпълнение на служебните им задължения. Като зони с контролиран достъп се определят всички помещения на територията на УЧЕБНОТО ЗАВЕДЕНИЕ, в които се събират, обработват и съхраняват лични данни.

Достъпът до системите, обработващи по електронен способ лични данни, е ограничен чрез уникални потребителски идентификатори и пароли, а електронните носители, са защитени по адекватен начин, в зони с контрол на достъпа.

Основните приложими технически мерки за физическа защита в УЧЕБНОТО ЗАВЕДЕНИЕ включват използване на ключалки, шкафове, метални каси, както и оборудване на помещенията с пожарогасителни средства.

Основните мерки на персоналната защита са:

1. познаване на нормативната уредба в областта на защитата на личните данни;

2. познаване на политиката и ръководствата за защита на личните данни;

3. знания за опасностите за личните данни, обработвани от администратора;

4. споделяне на критична информация между персонала (например идентификатори, пароли за достъп и т.н.);

5. съгласие за поемане на задължение за неразпространение на личните данни.

6. Мерките за персонална защита гарантират достъпа до лични данни само на лица, чиито служебни задължения или конкретно възложена задача налагат такъв достъп.

7. Личните данни се събират само с конкретна цел, пряко свързана с изпълнение на законовите задължения и/или нормалната дейност на УЧЕБНОТО ЗАВЕДЕНИЕ, а начинът на тяхното съхранение се съобразява със специфичните нужди за обработка;

8. Достъпът до регистрите е ограничен и се предоставя само на упълномощените служители.

9. Личните данни се съхраняват толкова дълго, колкото е необходимо, за да се осъществи целта, за която са били събрани и/или изискванията на действащото законодателство.

10. Документите, съдържащи лични данни, които не подлежат на издаване към Държавен архив, и след изтичане на законовите срокове за тяхното съхранение и не са

необходими за нормалното функциониране на УЧЕБНОТО ЗАВЕДЕНИЕ, се унищожават по подходящ и сигурен начин чрез изгаряне, нарязване, електронно изтриване и други подходящи за целта методи.

11. За всяко унищожаване на лични данни, което не е пряко свързана с изпълнение на законовите задължения и/или нормалната дейност на УЧЕБНОТО ЗАВЕДЕНИЕ, се документира.

Защитата на автоматизираните информационни системи и/или мрежи

УЧЕБНОТО ЗАВЕДЕНИЕ включва набор от приложими технически и организационни мерки за предотвратяване на нерегламентиран достъп до системите и/или мрежите, в които се създават, обработват и съхраняват лични данни.

1. Идентификация чрез използване на пароли за лицата, които имат достъп до мрежата и ресурсите на УЧЕБНОТО ЗАВЕДЕНИЕ. Прилагането на тази мярка е с цел да се регламентират нива на достъп;

2. Управление на регистрите, съобразено с ограничаване на достъпа до съответния регистър единствено до лица, които са пряко натоварени и/или служебно ангажирани с неговото въвеждане, поддръжка и обработка;

3. Защитата от вируси, включва използването на стандартни конфигурации за всяка компютърна и/или мрежова платформа, като системният, а при възможност и приложният, софтуер се контролира, инсталира и поддържа от избрано за целта лице.

4 Основни електронни носители на информация са: вътрешни твърди дискове, еднократно и/или многократно презаписваеми външни носители (външни твърди дискове, многократно презаписваеми карти, памети ленти и други носители на информация, еднократно записваеми носители и др.)

5. Личните данни в електронен вид се съхраняват съгласно нормативно определените срокове и съобразно спецификата и нуждите на УЧЕБНОТО ЗАВЕДЕНИЕ.

6. Данните, които вече не са необходими за целите на УЧЕБНОТО ЗАВЕДЕНИЕ и чийто срок за съхранение е изтекъл, се унищожават чрез приложим способ чрез нарязване, изгаряне или постоянно заличаване от електронните средства.

Базисни правила и мерки за осигуряване на защита на личните данни при компютърна обработка

1. Компютърен достъп към файлове, съдържащи лични данни, се осъществява само от длъжностни лица с регламентирани права, единствено от тяхното физическо работно място, от специално определения за целта компютър и след идентификация чрез парола.

2. С цел повишаване сигурността на достъпа до информация служителите задължително променят използваните от тях пароли на период от 6 месеца. В случай на отпадане на основанието за достъп до лични данни правата на съответните лица се преустановяват, включително и чрез изтриване на акаунта).

3. Използваният хардуер за съхранение и обработване на лични данни отговаря на съвременните изисквания и позволява възможности за архивиране и възстановяване на данните и работното състояние на средата.

4. При необходимост от ремонт на компютърната техника, предоставянето й на сервизната организация се извършва без устройствата, на които се съхраняват лични данни.

5. На служебните компютри се използва само софтуер, който е инсталиран от оторизирано лице. При внедряване на нов програмен продукт за обработване на лични данни се тестват и проверяват възможностите на продукта с оглед спазване изискванията на Закона за защита на личните данни и осигуряване максималната им защита от неправомерен достъп, загубване, повреждане или унищожаване.

6. Служителите, на които е възложено да подписват служебна кореспонденция с универсален електронен подпис (УЕП), нямат право да предоставят издадения им УЕП на трети лица.

УЧЕБНОТО ЗАВЕДЕНИЕ предприема превантивни действия при защита на личните данни като съставя план за действие при различните случаи на настъпили форсмажорни събития, а именно:

1. защита при аварии, независещи от УЧЕБНОТО ЗАВЕДЕНИЕ – предприемат се конкретни действия в зависимост от конкретната ситуация;

2. защита от пожари - незабавно гасене със собствени средства /пожарогасители/ и уведомяване на съответните органи;

3. защита от наводнения – предприемат се действия по ограничаване на разпространението, както и се изпомпва водата или загребва със собствени подръчни средства.

Служителите на УЧЕБНОТО ЗАВЕДЕНИЕ са длъжни:

1. да обработват лични данни законосъобразно и добросъвестно;

2. да използват личните данни, до които имат достъп, съобразно целите, за които се събират, и да не ги обработват допълнително по начин, несъвместим с тези цели;

3. да актуализират регистрите на личните данни (при необходимост);

4. да заличават или коригират личните данни, когато се установи, че са неточни или непропорционални по отношение на целите, за които се обработват;

5. да поддържат личните данни във вид, който позволява идентифициране на съответните физически лица за период не по-дълъг от необходимия за целите, за които тези данни се обработват.

6. да не разгласяват лични данни, до които са получили достъп при и по повод изпълнение на задълженията си.

7. За неспазването на разпоредбите на настоящата инструкция служителите носят административна отговорност.

8. Всички служители на УЧЕБНОТО ЗАВЕДЕНИЕ са длъжни срещу подпис да се запознаят с инструкцията и да я спазват.