ПРОФЕСИОНАЛНА ГИМНАЗИЯ ПО ГОРСКО СТОПАНСТВО И ДЪРВООБРАБОТВАНЕ "НИКОЛАЙ ХАЙТОВ" - ГР.ВАРНА

З А П О В Е Д

№ РД-08-0295

гр.Варна, 25.09.2020г.

Във връзка с разпоредбите на Закона за защита на личните данни и изискванията на Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни (Общ регламент относно защитата на личните данни), както и с чл. 257, ал. 1, чл. 258, ал.1 и чл. 259, ал. 1 от Закона за предучилищното и училищното образование, с цел създаване на ясни процедури и механизми с оглед изискванията за прозрачност при съобразяване с механизмите за защита на личните данни; определянето на видовете регистри, които се водят в гимназията; определянето на правата и задълженията на лицата, обработващи лични данни и/или лицата, които имат достъп до лични данни и работят под ръководството на обработващите лични данни; определянето на отговорността при неизпълнение на тези задължения и с цел създаването на процедури за докладване, управление и реакция при инциденти по време на образователно-възпитателния процес и останалата дейност на гимназията,

У Т В Ъ Р Ж Д А В А М

Вътрешни правила за мрежова и информационна сигурност на ПГГСД „Николай Хайтов", гр.Варна.

инж. МАРИЯ ГЕОРГИЕВА

Директор на ПГГСД "Н. Хайтов"
гр. Варна

ВЪТРЕШНИ ПРАВИЛА ЗА МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ НА ПГГСД „НИКОЛАЙ ХАЙТОВ“ ГР.ВАРНА

I.ОБЩИ ПОЛОЖЕНИЯ

Чл. 1. Настоящите вътрешни правила се утвърждават на основание чл. 1, ал. 1, т. 5 от Наредбата за минималните изисквания за мрежова сигурност, приета с ПМС № 186 от 26.07.2019 г., и имат за цел осигуряването на контрол и управление на работата на информационните системи в ПГГСД „Николай Хайтов“ гр.Варна.

Чл. 2. В ПГГТСД „Николай Хайтов“ гр. Варна се прилагат организационни и технически мерки за защита, които да гарантират нормативноустановените принципи на обработване на лични данни – законосъобразност, добросъвестност, прозрачност, точност и съвместимост с целите и мерките за изпълнение и прилагане на 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), (ОВ, L119/1 от 4 май 2016 г.), наричан по нататък „Регламент (ЕС) 2016/679“ и Закона за защита на личните данни.

II.АДМИНИСТРАТОР И ОБРАБОТВАЩИ ЛИЧНИ ДАННИ

Чл. 3. Администратор на лични данни е ПГГТСД „Николай Хайтов“ гр.Варна - юридическо лице на бюджетна издръжка със седалище гр. Варна.

Чл. 4. ПГГСД „Николай Хайтов“ гр.Варна обработва личните данни самостоятелно.

Чл. 5. (1) Достъпът и обработването на лични данни се осъществява само от лица, чиито служебни задължения (по длъжностна характеристика) или конкретно възложена задача налагат такъв достъп, при спазване на принципа „Необходимост да знае“.

(2) Служителите на ПГГТСД „Николай Хайтов“ гр.Варна, са длъжни да познават нормативната уредба в областта на защитата на личните данни, включително и Регламент (ЕС) 2016/679, настоящите Вътрешни правила, както и рисковете за правата и свободите на физическите лица, чиито лични данни се обработват в ПГГТСД „Николай Хайтов“ гр.Варна, като за целта подписват декларация или се задължават с длъжностната характеристика да не разгласяват личните данни, до които са получили достъп при и по повод изпълнение на задълженията си.

Чл. 6. При неспазването на ограниченията за достъп до личните данни и

нарушаване на задълженията за спазване на конфиденциалност, цялостност и наличност на обработваните лични данни служители на ПГТСД „Николай Хайтов“ гр.Варна, носят дисциплинарна отговорност.

III.ЗАДЪЛЖЕНИЯ НА АДМИНИСТРАТОРА НА ЛИЧНИ ДАННИ

Чл. 7. В случай на нарушение на сигурността на личните данни, служителите на гимназията са длъжни незабавно след узнаването да уведомят директора на ПГТСД „Николай Хайтов“ гр. Варна, който е длъжен да уведоми КЗЛД за нарушението на сигурността на личните данни не по-късно от 72 часа, след узнаването, освен ако не съществува вероятност нарушението на сигурността на личните данни да породи риск за правата и свободите на физическите лица.

Чл. 8. Когато нарушението на сигурността на личните данни има вероятност да породи висок риск за правата и свободите на физическите лица, служителите на гимназията без ненужно забавяне, съобщават на субекта на данните за нарушението на сигурността на личните данни, освен когато:

1. са предприети подходящи мерки за защита, и тези мерки са приложени по отношение на личните данни, засегнати от нарушението;

2. са взети впоследствие мерки, които гарантират, че вече няма вероятност да се материализира високият риск за правата и свободите на субектите на данни;

3. това би довело до непропорционални усилия.

Чл. 9. Администраторът на лични данни осигурява необходимите финансови, технически и човешки ресурси за определянето и въвеждането на подходящи организационни и технически мерки, за защита на личните данни.

Чл. 10. Директорът на ПГТСД “Николай Хайтов“ гр.Варна определя служители на гимназията, със следните отговорности:

1. извършване на предварителен и последващ контрол на материалите, публикувани в интернет сайта/страницата на ПГТСД “Николай Хайтов“ гр.Варна, находяща се в Глобалната информационна мрежа - Интернет, на адрес www.pggsd-varna.com, за съответствие с нормативната уредба в областта на защитата на личните данни;

2. извършване на преглед и предприемане на действия за актуализиране на договорености с обработващите лични данни, декларациите, и другите форми на документиране на съгласието на субекта на данни, както и на декларациите и длъжностните характеристики на служителите;

3. извършване на периодични проверки за необходимостта от съхраняване на обработваните лични данни;

4. изпитване за преценяване на ефективността на прилаганите технически и организационни мерки с оглед гарантиране на сигурността на обработваните лични

данни, поне два пъти годишно.

IV.ТЕХНИЧЕСКИ И ОРГАНИЗАЦИОННИ МЕРКИ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

Чл. 11. ПГТСД „Николай Хайтов“ гр.Варна, като администратор на лични данни осигурява чрез съответните служители подходящи технически и организационни мерки за осигуряване на ниво на сигурност, съобразено с рисковете за правата и свободите на физическите лица.

Чл. 12. В гимназията се поддържа актуален списък на обработваните категории лични данни и въведените технически и организационни мерки за защита.

Чл. 13. При оценката на подходящото ниво на сигурност се вземат предвид преди всичко рисковете, свързани с обработването като случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или достъп до обработвани лични данни.

Чл. 14. Мерките за защита могат да включват и псевдонимизация и криптиране на личните данни, способност за гарантиране на постоянна поверителност, цялостност, наличност и устойчивост на системите за обработване, способност за своевременно възстановяване на наличността и достъпа до лични данни в случай на физически или технически инцидент, процес на редовно изпитване, преценяване и оценка на ефективността на техническите и организационни мерки.

Чл. 15. (1) Подходящите технически и организационни мерки се въвеждат към момента на определяне на средствата за обработване и към момента на самото обработване.

(2) Задължението за въвеждане на подходящи мерки се отнася до обема на събраните лични данни, степента на обработването, периода на съхраняването им и тяхната достъпност.

Чл. 16. С мерките по предходния член администраторът на лични данни гарантира, че по подразбиране се обработват лични данни, които са необходими за всяка конкретна цел на обработването.

Чл. 17. В ПГТСД „Николай Хайтов“ Варна се прилагат следните минимални технически и организационни мерки за защита на личните данни:

1. Мерки за физическа защита - в зоната с контролиран достъп.

Чл. 18. (1) Физическа защита в ПГТСД „Николай Хайтов“ се осигурява чрез набор от приложими технически и организационни мерки за предотвратяване на нерегламентиран достъп и защита на сградите и помещенията, в които се обработват и съхраняват лични данни.

(2) Основните приложими организационни мерки за физическа защита включват определяне на помещенията, в които ще се обработват лични данни, както и на тези, в които ще се разполагат елементите на комуникационно-информационните системи за обработване на лични данни, вкл. и определяне на организацията на физическия достъп.

(3) 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.

(4) Когато в тези помещения имат достъп и външни лица, в помещенията се обособява непублична част, която е физически ограничена и достъпна само за служители, на които е необходимо да имат достъп с оглед изпълнението на служебните им задължения.

(5) Комуникационно-информационните системи, използвани за обработка на лични данни, се разполагат в помещения, достъпът до които е ограничен само до тези служители, които за изпълнение на служебните си задължения се нуждаят от такъв достъп до данните, както и лицата, натоварени със служебни ангажименти за поддръжката на нормалното функциониране на тези системи. Последните нямат достъп до съхраняваните в електронен вид данни.

(6) Организацията на физическия достъп до помещения, в които се обработват лични данни, е базирана на ограничен физически достъп (на база заключващи системи). Достъп се предоставя само на служителите, на които той е необходим, за изпълнение на служебните им задължения.

(7) Като зони с контролиран достъп се определят всички помещения на територията на ПГГСД „Николай Хайтов“, в които се събират, обработват и съхраняват лични данни.

(8) 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.

(9) Основните приложими технически мерки за физическа защита в ПГГСД „Николай Хайтов“ включват използване на ключалки, шкафове, метални каси, както и оборудване на помещенията с пожарогасителни средства.

а) ПГГСД „Николай Хайтов“ гр.Варна обработва личните данни в обект на адрес: гр.Варна, ул.“Орех“ No11;

б) кабинетите са разположени в масивна сграда;

в) входните врати на кабинетите са масивни, със секретна брава;

г) в сградата има пропускателен режим;

д) личните данни се обработват в кабинетите на определените от директора на гимназията служители;

е) елементите на комуникационно-информационните системи (КИС), използвани за обработване на лични данни се намират в охраняема зона;

ж) всички документи на хартиен носител, съдържащи лични данни, се съхраняват в заключени шкафове в съответния кабинет, с ограничен достъп само за упълномощени лица;

з) помещенията, в които се обработват лични данни са оборудвани със заключващи се врати, заключващи се метални шкафове и/или каси, пожароизвестителна система и пожарогасителни средства;

и) достъп до помещенията, в които се обработват лични данни имат определените за целта лица - външни лица не се допускат;

й) до зоната с контролиран достъп се допускат лица, след проверка на документ за самоличност или служебна карта.

2. Мерки за персонална защита.

а) достъпът до лични данни се осъществява само от лица, чиито служебни задължения или конкретно възложена задача налагат такъв достъп, при спазване на принципа „Необходимост да знае“;

б) всички служители са длъжни да спазват ограниченията за достъп до личните данни, и са персонално отговорни пред администратора за нарушаването на принципите за „Поверителност“, „Цялостност“ и „Наличност“ на личните данни.

в) лицата, обработващи лични данни, при постъпване на работа се запознават с:

аа) нормативната уредба в областта на защита на личните данни и актовете по нейното прилагане;

бб) опасностите за личните данни, обработвани от администратора;

вв) вътрешните правила на администратора.

г) най-малко веднъж годишно се провежда обучение за защита на личните данни.

бб) споделяне на критична информация между служителите (като идентификатори, пароли за достъп и т.н.) е строго забранено.

3.Мерки за документална защита.

а) при осъществяване на дейности по управление на човешки ресурси се обработват лични данни на хартиен носител (кадрови досиета, чието съдържание съответства на нормативната уредба в Република България, както и на вътрешните

нужди за периодична оценка на служителите, и др.).

б) досиетата по буква „а“ се съхраняват в заключващи се шкафове в зона с ограничен достъп.

в) обработването на лични данни на хартиен носител се извършва само в работно време, по изключение в извън работно време - след разпореждане на директора на гимназията.

г) достъп до регистрите имат служителите в съответствие с принципа „Необходимост да знае“.

д) контрол на достъпа до регистрите се упражнява от директора на гимназията или от определено от него длъжностно лице.

е) сроковете за съхранение на данните са определени поотделно за всяка дейност по обработване.

ж) за унищожаване на лични данни директорът на гимназията назначава комисия;

з) документите, съдържащи лични данни се унищожават по начин, непозволяващ тяхното възстановяване.

и) след унищожаването на документите комисията по буква „ж“ съставя протокол и го представя на директора на гимназията за утвърждаване.

й) личните данни могат да бъдат размножавани и разпространявани от упълномощените служители, само ако е необходимо за изпълнение на служебни задължения или ако са изискани по надлежния ред от упълномощени за това лица.

4. Защита на автоматизирани информационни системи и/или мрежи (АИС/М).

а) личните данни, обработвани в ПГТСД “Николай Хайтов“ гр. Варна, подлежат на електронна обработка.

б) електронната обработка се реализира с помощта на специализирани приложни софтуерни продукти и чрез стандартни средства за текстообработка, електронни таблици и др. (офис-пакети).

в) при електронната обработка се използват само лицензирани системни и приложни софтуерни продукти или компютърни програми и бази данни, създадени в рамките на трудово правоотношение по реда на Закона за авторското право и сродните му права.

г) служителите, обработващи лични данни, задължително трябва да притежават необходимата компютърна грамотност и умение за работа с използваните специализирани софтуерни продукти.

д) всеки упълномощен потребител на АИС/М има личен профил с определени нива на достъп, съобразни с неговите задължения и принципа

„Необходимост да знае“.

е) идентификацията и автентификацията на потребителите се реализира със средствата на операционната система и на използваните специализирани софтуерни продукти чрез потребителско име и парола.

ж) сроковете за съхранение на данните са определени съобразно съответната дейност по обработване.

з) заличаването на личните данните в електронен вид се осъществява чрез стандартните средства на операционната система или със средствата на специализираните софтуерни продукти.

и) с цел възстановяване на данните от регистрите се поддържат резервни копия за възстановяване на базите данни и на данните във файловата система.

й) за помещенията, в които са разположени компютърни и комуникационни средства, е осигурено заключване на помещенията, система за ограничаване на достъпа.

к) работните компютърни конфигурации, както и цялата IT инфраструктура, включително и достъпът до интернет, се използват единствено за служебни цели.

л) забранено е използването на преносими носители на данни за лични нужди.

м) не се разрешава осъществяването на отдалечен достъп до данни от регистрите.

н) за защита на данните е инсталирана антивирусна програма и се извършва седмична профилактика на софтуера и системните файлове.

о) за поддържането на АИС/М се определят системни администратори от ПГГСД “Николай Хайтов“.

п) администраторът на АИС/М създава и поддържа базови конфигурации за защита на операционната система, защитни стени, рутери и мрежови устройства, както и следи за своевременно обновяване (update) на системния, технологичния (офис-пакети и др.), приложния и антивирусния софтуер.

5. Мерки за криптографска защита.

а) за криптографска защита се използват стандартните криптографски възможности на операционната система, на системите за управление на бази данни, на комуникационното оборудване, както и квалифицирани електронни подписи (КЕП).

V.ДЕЙСТВИЯ ЗА ЗАЩИТА ПРИ АВАРИИ, ПРОИЗШЕСТВИЯ И БЕДСТВИЯ (ПОЖАР, НАВОДНЕНИЕ И ДР.)

Чл. 19. При възникване и установяване на инцидент веднага се докладва на директора на гимназията и в зависимост от обстоятелствата се уведомяват

съответните компетентни институции.

Чл. 20. С наличните ресурси се вземат мерки за ограничаване въздействието върху регистрите, ако това е възможно.

Чл. 21. (1) За инцидентите се води дневник, в който задължително се вписват предполагаемото време или период на възникване, времето на установяване, времето на докладване и името на служителя, извършил доклада.

(2) След анализ на инцидента, упълномощено лице вписва в дневника последствията от инцидента и мерките, които са предприети за отстраняването им.

Чл. 22. В случаите на необходимост от възстановяване на данни, процедурата се изпълнява след писменото разрешение на директора на гимназията.

VI. ПРЕДОСТАВЯНЕ НА ЛИЧНИ ДАННИ НА ТРЕТИ ЛИЦА

Чл. 23. Лични данни, обработвани от администратора, се предоставят на държавни органи единствено в изпълнение на задължения, произтичащи от нормативни актове.

Чл. 24. Данни, обработвани при осъществяване на дейност по управление на човешки ресурси, могат да бъдат предоставяни на държавни институции с оглед изпълнение на нормативно задължение (например на съда, прокуратурата, НОИ, НАП, МВР и др.).

Чл. 25. В качеството си на работодател, в случаите и по ред, предвидени в закон, директорът на гимназията предоставя лични данни на персонала и на определени кредитни институции (например банки), във връзка с изплащането на дължимите възнаграждения на служители, изпълнители по граждански договори, кредитни задължения и др.

VII. РЕД ЗА ИЗПЪЛНЕНИЕ НА ЗАДЪЛЖЕНИЯТА НА АДМИНИСТРАТОРА СЛЕД ПОСТИГАНЕ ЦЕЛТА НА ОБРАБОТВАНЕ НА ЛИЧНИТЕ ДАННИ ИЛИ ПРЕДИ ПРЕУСТАНОВЯВАНЕ НА ОБРАБОТВАНЕТО НА ЛИЧНИТЕ ДАННИ

Чл. 26. При преустановяване на обработването на личните данни в регистрите, администраторът на лични данни е длъжен да ги унищожи, или да ги прехвърли на друг администратор.

Чл. 27. След изтичане на срока за съхранение на данните комисия, назначена от директора на гимназията, определя кои документи подлежат на унищожение, начина и мястото на извършване на процедурата.

Чл. 28. При унищожаването на данните от регистрите се съставя протокол.

Чл. 29. При прехвърляне на данните от регистрите на друг администратор се оформя двустранен протокол.

Чл. 30. След постигане целта на обработване на личните данни директорът

на гимназията ги съхранява само в предвидените в закон случаи.

Чл. 31. Администраторът на лични данни може да възложи на друг администратор на лични данни да извърши процедурата по унищожаване на документи.

Чл. 32. В писмения акт по възлагането се определят правата и задълженията на изпълнителя във връзка с унищожаване на документите.

Чл. 33. Унищожаването на данните на хартиен или магнитен носител се извършва по начин, непозволяващ тяхното възстановяване, например чрез разрязване с помощта на машина - шредер и/или чрез изгаряне или разрушаване (отваряне) на корпуса и разтрошаване на носителя на данни и др.

Чл. 34. Информационните носители предварително се проверят, за да е сигурно, че необходимата информация е копирана и след това цялата информация е изтрита от тях преди унищожаване.

Чл.35 Забранява се свързването на компютри едновременно в мрежата на ПГГСД "Николай Хайтов" и в други мрежи, когато това позволява разкриване и достъп до IP адреси от мрежата на ПГГСД "Николай Хайтов" и/или е в противоречие с изискванията на Наредбата за минималните изисквания за мрежова и информационна сигурност.

Чл.36 Забранява се инсталирането и използването на комуникатори (като skype, facebook, messenger, viber и др. подобни), осигуряващи достъп извън рамките на компютърната мрежа на ПГГСД "Николай Хайтов" и създаващи предпоставки за идентифициране на IP адрес на потребителя и за достъп на злонамерен софтуер и мобилен код до компютрите, свързани в компютърната мрежа на ПГГСД "Николай Хайтов".

Чл.37 Забранява се съхраняването на компютрите на ПГГСД "Николай Хайтов" на лични файлове с текст, изображения, видео и аудио.

Чл.38 Забранява се отварянето без контрол от страна на системния администратор:

1. получени по електронна поща или на преносими носители изпълними файлове, файлове с мобилен код и файлове, които могат да предизвикат промени в системната конфигурация, напр. файлове с разширения .exe, .vbs, .reg и архивни файлове;

2. получени по електронна поща съобщения, които съдържат неразбираеми знаци.

Чл.39 С цел антивирусна защита се прилагат следните мерки:

1. Всички персонални компютри имат инсталиран антивирусен софтуер в реално време, който се обновява редовно.

Чл.40 Архивирането на данните се извършва по начин, който позволява, при необходимост данните да бъдат инсталирани на друг компютър и да се продължи работният процес без чувствителна загуба на данни.

ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§ 1. Контролът по спазване на правилата се осъществява от ръководството на ПГТСД "Николай Хайтов".

§ 2. Настоящите вътрешни правила се разглеждат и оценяват периодично с оглед ефективността им, като ПГТСД "Николай Хайтов" може да приема и прилага допълнителни мерки и процедури, които са целесъобразни и необходими с оглед защитата на информацията.

§ 3. Тези правила са разработени съгласно Наредбата за минималните изисквания за мрежова сигурност (приета с ПМС № 186 от 26.07.2019 г.) и влизат в сила от датата на извеждане на Заповед №РД-08-0295/25.09.2020г. на Директора на ПГТСД "Николай Хайтов".