ПРОФЕСИОНАЛНА ГИМНАЗИЯ ПО ЕЛЕКТРОПРОМИШЛЕНОСТ И ТЕКСТИЛ „ЗАХАРИ СТОЯНОВ"
6450, гр. Харманли, ул. „Любен Каравелов" № 1, E-mail: pget@abv.bg http://pget-harmanli.com
тел.: Директор - 0373 85068; 0879171464; Техн.секретар – 0879374209; Гл. счетоводител - 0895393666

ЗАПОВЕД
№ 442/13.02.2023 г.

На основание чл. 259, ал. 1 от Закона за предучилищното и училищното образование и чл. 33 и 34 от Регламента (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. и във връзка с необходимостта от защитата на физическите лица при обработването на лични данни

I. УТВЪРЖДАВАМ:

1. Инструкция за действие при пробив в сигурността на личните данни с приложения, както следва:
   1.1. Методология за оценка на тежестта на пробив в сигурността на личните данни;
   1.2. Уведомление до надзорния орган;
   1.3. Съобщение до субекта на данните за нарушение на сигурността на личните данни;
   1.4. Регистър на нарушения на сигурността на личните данни.

II. НАРЕЖДАМ:

2. В срок до десет работни дни от издаването на настоящата заповед, утвърдената Инструкция за действие при пробив в сигурността на личните данни с приложенията ѝ да се доведе до знанието на служителите в институцията за сведение и изпълнение, което се удостоверява лично с подпис.

3. Изпълнението по т. 2 възлагам на длъжностното лице по защита на данните.

4. За неизпълнение на разпоредбите на утвърдената Инструкция за действие при пробив в сигурността на личните данни с приложенията ѝ, виновните лица носят дисциплинарна отговорност.

5. Контролът по изпълнението на заповедта възлагам на Светлана Николова, заместник-директор.

Соня Илиева
Директор на ПГЕТ „Захари Стоянов", гр. Харманли

Приложение № 1

Посочени в Приложение 2 от Насоки относно оценката на въздействието върху защитата на данните (ОВЗД) и определяне дали съществува вероятност обработването „да породи висок риск" за целите на Регламент (ЕС) 2016/679, приети от Работната група за защита на личните данни по чл. 29, WP 248, rev 1

Критерии за приемлива оценка на въздействието върху защитата на данните

Работна група 29[1] предлага следните критерии, които администраторите могат да използват, за да оценят дали оценката на въздействието върху защитата на данните (ОВЗД) или методология за извършване на ОВЗД е достатъчно всеобхватна, така че да отговаря на ОРЗД (Общ регламент относно защитата на данните):

□ осигурен е системен опис на обработването (член 35, параграф 7, буква „а" от **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), наричан по-долу Регламент (ЕС) 2016/679:**

□ вземат се предвид естеството, обхватът, контекстът и целите на обработването (съображение 90 от Регламент (ЕС) 2016/679);

□ поддържа се регистър на личните данни, получателите и срока, за който ще се съхраняват личните данни;

□ осигурено е функционално описание на операцията по обработване;

□ определени са елементите, свързани с личните данни (хардуер, софтуер, мрежи, лица, хартиен носител или канали за предаване на хартиен носител);

□ взема се предвид спазването на одобрени кодекси за поведение (член 35, параграф 8 от Регламент (ЕС) 2016/679);

□ оценяват се необходимостта и пропорционалността (член 35, параграф 7, буква „б" от Регламент (ЕС) 2016/679):

□ определени са мерки за спазване на Регламента (член 35, параграф 7, буква „г" и съображение 90 от Регламент (ЕС) 2016/679), като се вземат предвид:

□ мерки, допринасящи за пропорционалността и необходимостта на обработването въз основа на:

• конкретна, изрично указана и легитимна цел или цели (член 5, параграф 1, буква „б" от Регламент (ЕС) 2016/679);

• законосъобразност на обработването (член 6 от Регламент (ЕС) 2016/679);

• подходящи, свързани със и ограничени до необходимото данни (член 5, параграф 1, буква „в" от Регламент (ЕС) 2016/679); • ограничена продължителност на съхранението (член 5, параграф 1, буква „д" от Регламент (ЕС) 2016/679);

□ мерки, допринасящи за правата на субектите на данни:

• информиране на субекта на данни (членове 12, 13 и 14 от Регламент (ЕС) 2016/679);
• право на достъп и на преносимост на данните (членове 15 и 20 от Регламент (ЕС) 2016/679);
• право на коригиране и на изтриване (членове 16, 17 и 19 от Регламент (ЕС) 2016/679);
• право на възражение и на ограничаване на обработването (членове 18, 19 и 21 от Регламент (ЕС) 2016/679);
• взаимоотношения с обработващите лични данни (член 28 от Регламент (ЕС) 2016/679);
• гаранции при международно предаване на данни (глава V от Регламент (ЕС) 2016/679);
• предварителна консултация (член 36 от Регламент (ЕС) 2016/679).

□ управляват се рисковете за правата и свободите на субектите на данни (член 35, параграф 7, буква „в" от Регламент (ЕС) 2016/679)):

□ оценяват се произходът, естеството, спецификата и степента на рисковете (вж. съображение 84 от Регламент (ЕС) 2016/679), или по-конкретно за всеки риск, (незаконен достъп, нежелани изменения и изчезване на данни) от гледна точка на субектите на данни:

• вземат се предвид източниците на риска (съображение 90 от Регламент (ЕС) 2016/679);

• определят се потенциалните въздействия върху правата и свободите на субектите на данни в случай на определени събития, включително незаконен достъп, нежелани изменения и изчезване на данни;

• определят се заплахи, които биха могли да доведат до незаконен достъп, нежелани изменения и изчезване на данни;

• изчисляват се вероятността и тежестта (съображение 90 от Регламент (ЕС) 2016/679);

• определят се мерки за третиране на тези рискове (член 35, параграф 7, буква „г" от Регламент (ЕС) 2016/679) и съображение 90 от него);

□ заинтересованите страни участват:

□ иска се становището на главния служител по сигурността на информацията (ГССИ) [2] (член 35, параграф 2 от Регламент (ЕС) 2016/679);

□ по целесъобразност се търсят становищата на субектите на данни или техните представители (член 35, параграф 9 от Регламент (ЕС) 2016/679).

[1] Сега Европейски комитет по защита на данните

[2] В образователните институции няма Главен служител по сигурността на информацията, тъй като нямат такива звена, поради общата приложимост на критериите и за яснота е посочен

Изх. № ……/……..

Приложение № 2

ДО
КОМИСИЯТА ЗА ЗАЩИТА
НА ЛИЧНИТЕ ДАННИ
София, 1592
бул., „Проф. Цветан Лазаров“ № 2

УВЕДОМЛЕНИЕ ЗА НАРУШЕНИЕ НА СИГУРНОСТТА НА ЛИЧНИТЕ ДАННИ
НА ОСНОВАНИЕ ЧЛ. 33, ПАР. 1 ОТ РЕГЛАМЕНТ (ЕС) 2016/679
от Професионална гимназия по електропромишленост и текстил "Захари Стоянов"

УВАЖАЕМИ ГОСПОДИН ДИРЕКТОР/УВАЖАЕМА ГОСПОЖО ДИРЕКТОР,

Във връзка с установено нарушение на сигурността на обработвани от нас лични данни, в изпълнение на чл. 33 от Регламент (ЕС) 2016/679 (Общ регламент относно защитата на данните), Ви уведомяваме за следното нарушение на сигурността на личните данни:

1. Данни за нарушението

Описание на естеството на нарушението	
Категории засегнати субекти на данни и техният приблизителен брой	
Категории засегнати лични данни и приблизително количество на засегнатите записи	
Дата и час на установяване на нарушението	
Други обстоятелства относно нарушението	

2. Име и координати за връзка с длъжностното лице по защита на данните (или друга точка за контакт, от която може да се получи повече информация)

Име на длъжностното лице по защита на данните или друга точка за контакт	
Координати за връзка	

3. Описание на евентуалните последици от нарушението, според категориите лични данни

Нарушението на сигурността би могло да доведе до следните последици ……

…… *(описват се евентуалните неблагоприятни последици от нарушението, както и евентуалните рискове върху правата и свободите на субектите на данни)*

4. Описание на предприетите или предложените мерки за справяне с нарушението на сигурността на личните данни

За справяне с нарушението на сигурността на личните данни са предприети следните действия: ……

…… *(опишете предприетите действия по подаване на уведомлението на КЗЛД)*

За намаляване на евентуални неблагоприятни последици от нарушението на сигурността са предприети/планирани следните действия …… *(опишете, ако е приложимо за случая)*

5. Причини за забавяне на уведомлението *(посочва се само в случай, че уведомлението до надзорния орган е подадено по-късно от 72 часа от узнаване на нарушението на сигурността на личните данни)*

Причините настоящото уведомление да бъде подадено извън срока по чл. 33, пар. 1 от Регламент (ЕС) 2016/679 са следните: …….. *(описание на причините за забавянето)*

С уважение:

Соня Илиева,

Директор на ПГЕТ „Захари Стоянов"

гр. Харманли

Приложение № 3

Изх. № ..../.....

ДО

..... *(посочва се субектът на данни)*

СЪОБЩЕНИЕ ЗА НАРУШЕНИЕ НА СИГУРНОСТТА НА ЛИЧНИТЕ ДАННИ
НА ОСНОВАНИЕ ЧЛ. 34, ПАР. 1 ОТ РЕГЛАМЕНТ (ЕС) 2016/679
от Професионална гимназия по електропромишленост и текстил "Захари Стоянов"

УВАЖАЕМИ ГОСПОДИН ДИРЕКТОР/УВАЖАЕМА ГОСПОЖО ДИРЕКТОР

Във връзка с установено нарушение на сигурността на обработвани от нас лични данни, което може да породи висок риск за Вашите права и свободи като засегнат субект на данни, в изпълнение на чл. 34, пар. 1 от Регламент (ЕС) 2016/679 (Общ регламент относно защитата на данните), Ви предоставяме следната информация:

1. Естество на нарушението на сигурността на личните данни

Нарушението на сигурността, което засяга Ваши лични данни, се изразява в ..... *(описва се естеството на нарушението, засегнатите от него лични данни и причините, поради които се очаква висок риск за правата и свободите на субекта на данни)*

2. Име и координати за връзка с длъжностното лице по защита на данните (или друга точка за контакт, от която може да се получи повече информация)

Име на длъжностното лице по защита на данните или друга точка за контакт	
Координати за връзка	

3. Описание на евентуалните последици от нарушението, според категориите лични данни

Нарушението на сигурността би могло да доведе до следните последици ……. *(описват се евентуалните неблагоприятни последици от нарушението, както и евентуалните рискове върху правата и свободите на субектите на данни)*

4. Описание на предприетите или предложените мерки за справяне с нарушението на сигурността на личните данни

За справяне с нарушението на сигурността на личните данни са предприети следните действия: …… *(описват се предприетите действия)*

За намаляване на евентуални неблагоприятни последици от нарушението на сигурността са предприети/планирани следните действия …… *(опишете, ако е приложимо за случая)*

В случай, че имате допълнителни въпроси във връзка с нарушението на сигурността на личните Ви данни, не се колебайте да се свържете с нас, като използвате посочените по-горе координати за връзка.

С уважение:

Соня Илиева,

Директор на ПГЕТ „Захари Стоянов"

гр. Харманли

Приложение № 4

РЕГИСТЪР НА НАРУШЕНИЯТА НА СИГУРНОСТТА НА ЛИЧНИТЕ ДАННИ

№	Регистър с лични данни	Естество на нарушението	Място на нарушението	Време на възникване на нарушението	Време на узнаване за нарушението	Категории лични данни/ брой записи	Категории субекти на данни	Субекти на данни в други държави	Носители на данни	Уведомление до надзорния орган	Съобщения до субектите на данни	Причини за забавяне	Неблагоприятни последици	Предприети мерки
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1														

1. **Графа 1** служи за създаване на номерация на нарушенията, валидна за структурата на администратора.

2. В **графа 2** се посочва регистърът на лични данни, засегнат от нарушението.

3. В **графа 3** се отбелязва естеството на нарушението - изтриване, унищожаване и, загуба, промяна, неоторизиран достъп, разкриване, разпространяване или оповестяване на данни по друг начин, който ги прави достъпни без правно основание.

4. **Графа 4** служи за посочване на физическото място на възникване на нарушението.служи за посочване на физическото място на възникване на нарушението.

5. В **графа 5** се отразява предполагаемото време на възникване на нарушението.

6. В **графа 6** се отразява времето на узнаване за нарушението.

7. В **графа 7** се посочват категориите лични данни и приблизителния брой записи, засегнати от нарушението.

8. В **графа 8** се отразяват категориите субекти на данни, засегнати от нарушението и техния приблизителен брой.

9. В **графа 9** се посочват категориите субекти на данни в други държави, засегнати от нарушението и техния приблизителен брой.

10. В **графа 10** се отразяват носителите на данни, засегнати от нарушението – документи на хартиен носител, носители за многократен запис, автоматизирани информационни системи, аудиозаписи, видеозаписи и други.

11. В **графа 11** се отразява уведомлението до надзорния орган и датата, на която е направено.

12. В **графа 12** се посочва дали са направени съобщения за нарушения на сигурността на личните данни до субектите на данни

13. В **графа 13** се посочват причините за забавяне в сроковете за уведомяване.

14. **Графа 14** служи за отразяване на констатираните и/или очаквани неблагоприятни последици на нарушението.

15. В **графа 15** се отразяват предприетите технически и организационни мерки за справяне с нарушението и за намаляване на неблагоприятните му последици.