



УТВЪРЖДАВАМ:
ШИРИН ЕМИН – ГАРИБ
ДИРЕКТОР



ВЪТРЕШНИ ПРАВИЛА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

Глава първа

ОБЩИ ПОЛОЖЕНИЯ

Чл. 1. Вътрешните правила за защита на личните данни на Професионална гимназия по химични технологии и биотехнологии "Мария Кюри" определят прилаганите изисквания за защита на личните данни, реда за организация на задълженията за защита на личните данни и гарантирането на правата на субектите на данни, в съответствие с 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), Закона за защита на личните данни /ЗЗЛД/ и други правни изисквания за защита на данните, произтичащи от правото на Европейския съюз или от законодателството на Република България.

(2) Администраторът определя длъжностно лице по защита на данните и уведомява Комисията за защита на личните данни /КЗЛД/ за определеното длъжностно лице по защита на данните в съответствие с формата и съдържанието на уведомлението, утвърдени от КЗЛД. Администраторът публикува данните за контакт с длъжностното лице по защита на данните.

Чл. 3. В Професионална гимназия по химични технологии и биотехнологии "Мария Кюри" се прилагат всички принципи, свързани с обработването на лични данни, по чл. 5 от Регламент (ЕС) 2016/679, независимо в кой регистър с лични данни и на какво правно основание се осъществява обработването:

1. законосъобразност, добросъвестност и прозрачност;
2. ограничение на целите;
3. свеждане на данните до минимум;
4. точност;
5. ограничение на съхранението;
6. цялостност и поверителност;
7. отчетност.

Чл. 4. (1) 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 се знае“ и след запознаване с нормативната уредба в областта на защитата на личните данни и вътрешните правила, политики и процедури за защита на личните данни и опасностите за личните данни, обработвани от администратора.

(2) В длъжностните характеристики на служителите, работещи с лични данни, се предвиждат задължения за неразгласяване на данните, до които са получили достъп при или по повод изпълнение на длъжността.

Чл. 5. В Професионална гимназия по химични технологии и биотехнологии "Мария Кюри" обработваните лични данни са разпределени съгласно функционален принцип следните регистри с лични данни по смисъла на чл. 4, т. 6 от Регламент (ЕС) 2016/679:

1. Регистър „Деца/Ученици“;
2. Регистър „Човешки ресурси“;
3. Регистър „Предложения, сигнали, жалби и молби“;
4. Регистър „Контрагенти“;
5. Регистър „Видеонаблюдение и външни посетители“;
6. Регистър „Инициативи“;
7. Регистър „Болнични листовки“

Глава втора

ОПИСАНИЕ НА РЕГИСТРИТЕ С ЛИЧНИ ДАННИ

Чл. 6. (1) В регистър „Деца/Ученици“ се обработват лични данни на децата/учениците, кандидатстващи и приети в Професионална гимназия по химични технологии и биотехнологии "Мария Кюри", както и на техните родители/настойници/попечители и лични лекари с цел:

1. гарантиране на правото на образование;
2. изпълнение на нормативни изисквания, произтичащи от Закона за предучилищното и училищното образование, Закона за закрила на детето, Наредба № 8 от 11.08.2016 г. за информацията и документите за системата на предучилищното и училищното образование и други нормативни актове;

(2) Обработваните категории лични данни се отразяват в регистъра на дейностите по обработване на лични данни.

(3) Данните в регистър „Деца/Ученици“ се обработват на хартиен и технически носител.

(4) Данните в регистъра се предоставят от родителите или от настойниците/попечителите на децата/учениците при кандидатстване за прием в ПГХТБТ. Данните се въвеждат в изискуемите съобразно образователния стандарт за информацията и документите в системата на предучилищното и училищното образование.

(5) Данните от регистър „Деца/Ученици“ се обработват от директор, заместник-директори, учители, ЗАТС, счетоводители.

(6) Заместник-директорите са отговорни за контрола на достъпа до регистъра.

Чл. 7. (1) В регистър „Човешки ресурси“ се обработват лични данни на кандидатите за работа и на персонала, нает по трудови и извънтрудови правоотношения, с цел:

1. индивидуализиране на страните по трудови и извънтрудови правоотношения;
2. изпълнение на нормативните изисквания на Кодекса на труда, Кодекса за социално осигуряване, Закона за счетоводството, Закона за данъците върху доходите на физическите лица, Закона за Националния архивен фонд, Закона за предучилищното и училищното образование по отношение на обществените съвети и др.;
3. използване на събраните данни за:
 - а) всички дейности, свързани със съществуване, изменение и прекратяване на трудовите и извънтрудовите правоотношения;
 - б) изготвяне на всякакви документи на лицата в тази връзка;

в) установяване на връзка с лицето по телефон, за изпращане на кореспонденция, отнасяща се до изпълнение на задълженията му по трудовото или извънтрудовото правоотношение;

г) водене на счетоводна отчетност, удържане на дължими данъци и други дейности относно възнагражденията на посочените по-горе лица по трудови и извънтрудови правоотношения.

(2) Обработваните категории лични данни се отразяват в регистъра на дейностите по обработване на лични данни.

(3) Данните в регистър „Човешки ресурси“ се обработват на хартиен и технически носител.

(4) Данните в регистъра се предоставят от физическите лица при кандидатстване за работа, сключване на договор, избиране като членове на общественения съвет. Данните се въвеждат директно в договори, допълнителни споразумения, документи, удостоверяващи трудов стаж, служебни бележки, справки, удостоверения, кореспонденция и др.

(5) Данните от регистър „Човешки ресурси“ се обработват от ЗАТС, счетоводителите.

(6) Служителят „Човешки ресурси“ е отговорен за контрол на достъпа до регистъра.

Чл. 8. (1) В регистър „Предложения, сигнали, жалби и молби“ се обработват лични данни на лица, които сезират Професионална гимназия по химични технологии и биотехнологии "Мария Кюри" с молби, жалби, предложения и други подобни, с цел:

1. индивидуализиране на жалбоподателя, молителя, заявителя;

2. използване на събраните данни за установяване на връзка с лицето по телефон, за изпращане на кореспонденция, отнасяща се до молбата, жалбата, заявлението;

3. изпълнение на нормативни задължения.

(2) Обработваните категории лични данни се отразяват в регистъра на дейностите по обработване на лични данни.

(3) Данните в регистър „Предложения, сигнали, жалби и молби“ се обработват на хартиен и технически носител.

(4) Данните в регистъра се предоставят от физическите лица, за които се отнасят данните или от други лица в предвидените от нормативен акт случаи, като се съдържат в техните молби, предложения, жалби, заявления и приложения към тях или в документи, предоставяни от държавни органи и органи на местното самоуправление.

(5) Данните от регистър „Предложения, сигнали, жалби и молби“ се обработват от ЗАТС.

Чл. 9. (1) В регистър „Контрагенти“ се обработват лични данни на физически лица – изпълнители по граждански договори или представители на страните по договора, с цел:

1. индивидуализиране на страните по договора в преддоговорните и договорните отношения;

2. изпълнение на договора;

3. изпълнение на нормативни задължения във връзка с осчетоводяването и данъчното облагане на дейностите по договора.

(2) Обработваните категории лични данни се отразяват в регистъра на дейностите по обработване на лични данни.

(3) Данните в регистър „Контрагенти“ се обработват на хартиен и технически носител.

(4) Данните в регистъра се предоставят от физическите лица, за които се отнасят данните.

(5) Данните от регистър „Контрагенти“ се обработват от главния счетоводител и ЗАТС.

(6) Главният счетоводител на ПГХТБТ е отговорен за контрол на достъпа до регистъра.

Чл. 10. (1) В регистър „Видеонаблюдение и външни посетители“ се обработват лични данни на посетители в сградата на Професионална гимназия по химични технологии и биотехнологии "Мария Кюри" с цел:

1. подобряване на сигурността на децата/учениците и човешките ресурси и опазване на имуществото от посегателства;

2. гарантиране на обществения интерес при защитата на сигурността, живота и здравето на децата и учениците.

(2) Обработваните категории лични данни се отразяват в регистъра на дейностите по обработване на лични данни.

(3) Данните в регистър „Видеонаблюдение и външни посетители“ се обработват на хартиен и технически носител.

(4) Данните в регистъра се предоставят от физическите лица, за които се отнасят данните чрез преминаване на местата в обхвата на действие на средствата за видеонаблюдение.

Чл. 11. (1) В регистър „Инициативи“ се обработват лични данни на деца/ученици, техни близки, които участват в инициативи, организирани или провеждани в Професионална гимназия по химични технологии и биотехнологии "Мария Кюри", като например тържества, състезания, пътувания и други подобни, с цел:

1. индивидуализиране на желаещите да участват в инициативата;

2. публично оповестяване на данни за участниците с тяхно информирано и конкретно съгласие, при спазване и на другите изисквания на Регламент (ЕС) 2016/679 и чл. 25в от ЗЗЛД;

3. отчетност на дейностите по инициативата.

(2) Данните в регистъра се обработват на хартиен и технически носител.

(3) Данните в регистъра се предоставят от физическите лица, за които се отнасят данните и/или от техните родители, настойници или попечители.

(4) При необходимост от изготвяне на регламент, информационни материали или други подобни за съответната инициатива, проектите им се съгласуват с длъжностното лице по защита на данните с оглед съответствието им с изискванията за обработване на лични данни.

(5) Данните от регистъра се обработват от служителите, ангажирани с провеждането на съответната инициатива, при спазване на принципа „Необходимост да се знае“.

Чл. 12. (1) В зависимост от нормативното основание за събирането и предназначението им в регистрите се набират, обработва и съхраняват лични данни относно:

1. физическата идентичност на лицата – имена, ЕГН, номер на документ за самоличност, дата и място на издаването му, адрес, месторождение, телефони за контакт;

2. семейна идентичност на лицата – семейно положение, брой членове на семейството, родствени връзки и др.;

3. образование – вид на образованието, място, номер и дата на издаването на дипломата, допълнителна квалификация и др.;

4. трудова дейност – професионална биография, дни в осигуряване, осигурителен доход, основание за осигуряване, осигурени социални рискове, трудови договори, осигурители и други;

5. медицински данни – здраве статус, медицински диагнози и заключения на медицинската експертиза на временната и трайна неработоспособност;

6. други лични данни – осигурителен доход, трудови възнаграждения, парични обезщетения, статус на лицето (осъждано/неосъждано/реабилитирано) и други.

(2) Личните данни в регистрите се събират от администратора на лични данни на хартиен или електронен носител.

Чл. 13. Задълженията на лицето, отговарящо за водене и съхраняване на данните в регистъра (оправомощеното лице) включват набиране, обработване, актуализация и съхраняване на лични данни.

Чл. 14. Архивиране на личните данни на технически носител се извършва периодично всяка учебна година от обработващия лични данни, с оглед запазване на информацията за съответните лица в актуален вид.

Чл. 15. Контролът върху дейностите по обработка на лични данни се осъществява от лицето по защита на личните данни, определено от администратора. За ПГХТБТ „Мария Кюри“ това е Таня Маркова

Актуализация на лични данни

Глава трета

ДОСТЪП ДО ЛИЧНИ ДАННИ

1. ОСИГУРЯВАНЕ НА ДОСТЪП НА ЛИЦАТА ДО ЛИЧНИТЕ ИМ ДАННИ

Чл. 16. (1) Всяко физическо лице, както и служителите в училището, има право на достъп до отнасящите се до него лични данни, обработвани от администратора.

(2) В случаите, когато при осъществяване правото на достъп на физическото лице могат да се разкрият лични данни и за трето лице, администраторът предоставя на съответното физическо лице достъп само за частта от данните, отнасяща се него.

(3) При упражняване на правото си на достъп физическото лице има право по всяко време да поиска от администратора на лични данни:

1. Потвърждение за това, дали отнасящи се до него данни се обработват, информация за целите на това обработване, за категориите данни и за получателите или категориите получатели, на които данните се разкриват;

2. Съобщение до него в разбираема форма, съдържащо личните му данни, които се обработват, както и всяка налична информация за техния източник.

(4) При смърт на физическото лице право на достъп до личните му данни имат неговите наследници.

Чл. 17. (1) Правото на достъп се осъществява с писмена молба до администратора на лични данни.

(2) Молбата може да бъде отправена и по електронен път по реда на Закона за електронния документ и електронния подпис.

(3) Молбата по ал. 1 се отправя лично от физическото лице или от изрично упълномощено от него лице чрез нотариално заверено пълномощно.

Чл. 18. (1) Молбата по чл. 17 съдържа:

1. трите имена, ЕГН/ЛНЧ/, адрес за контакт и телефон на заявителя;
2. описание на искането;
3. предпочитана форма за предоставяне на достъп до личните данни;
4. подпис, дата на подаване на заявлението и адрес за кореспонденция.

(2) При подаване на молба от упълномощено лице, към същата се прилага и нотариално завереното пълномощно.

(3) При приемане на молбата, техническо лице извършва регистрацията на същата в деловодната система на администратора.

Чл. 19. (1) Физическото лице може да поиска копие на обработваните лични данни на предпочитан носител или предоставянето им по електронен път, освен в случаите, когато това е забранено от закон.

(2) Администраторът на лични данни е длъжен да се съобрази с предпочитаната от молителя форма на предоставяне на информацията по чл. 11, ал. 3.

(3) Администраторът на лични данни предоставя исканата информация във форма, различна от заявената, когато:

1. за исканата форма няма техническа възможност;
2. исканата форма е свързана с необосновано увеличаване на разходите по предоставянето.

Чл.20. (1) Администраторът на лични данни или изрично оправомощено от него лице разглежда молбата по чл.16 и се произнася в 14-дневен срок от неговото постъпване.

(2) Срокът по ал. 1 може да бъде удължен от администратора до 30 дни в случаите, когато обективно се изисква по-дълъг срок за събирането на всички искани данни и това сериозно затруднява дейността на администратора.

(3) С решението си администраторът предоставя пълна или частична информация на заявителя или мотивирано отказва предоставянето ѝ.

Чл.21. Право на достъп до данните в поддържаните от администратора регистри на лични данни имат служителите в ПГХТБТ „Мария Кюри“ – администратори на базите данни, служителите, на които е възложено приемането и обработването на лични данни върху хартиен и електронен носител (обработващите лични данни), както и служителите, за които служебните им функции налагат такъв достъп.

Чл.22. Служителите в ПГХТБТ „Мария Кюри“ с оторизиран достъп до лични данни са длъжни да обработват същите законосъобразно и добросъвестно, съобразно целите, за които се събират и да не ги обработват допълнително по начин, несъвместим с тези цели, както и да ги поддържат във вид, който им позволява идентифициране на съответните физически лица за период не по- дълъг от необходимия за целите, за които се обработват.

2. ДОСТЪП НА ТРЕТИ ЛИЦА ДО РЕГИСТРИТЕ СЪДЪРЖАЩИ ЛИЧНИ ДАННИ

Чл.23. (1) Достъп до обработваните от администратора лични данни имат лицата, за които същия произтича от законово или договорно основание, както и органи по надзора или на съдебната власт (Комисия за финансов надзор, съд, прокуратура, следствени органи и др.). Достъпът на тези органи до личните данни на лицата е правомерен.

(2) Не се изисква съгласие на лицето, ако обработването на неговите лични данни се извършва само от или под контрола на компетентен държавен орган за лични данни, свързани с извършване на престъпления, на административни нарушения и на непозволенни увреждания. На такива лица се осигурява достъп до личните данни, като при необходимост им се осигуряват съответни условия за работа в помещение на училището.

(3) Правомерен е и достъпът на ревизиращите държавни органи, надлежно легитимирани се със съответни документи – писмени разпореждания на съответния орган, в които се

посочва основанието, имената на лицата, като за целите на дейността им е необходимо да им се осигури достъп до кадровите досиета на персонала или клиентите.

(4) Решението си за предоставяне или отказване достъп до лични данни за съответното лице администраторът съобщава на третите лица в 30-дневен срок от подаване на молбата, респ. искането.

Глава четвърта

ВИДОВЕ ЗАЩИТА НА ЛИЧНИ ДАННИ

1. ЛИЦАТА ПО ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

Чл.24. (1) За обезпечаване на адекватна защита на регистрите с лични данни администраторът определя лице/лица по защита на личните данни.

(2) Лицето/лицата по защита на личните данни има следните правомощия:

1. Осигурява организация по водене на регистрите и мерки за гарантиране на адекватна защита;

2. Следи за спазването на конкретните мерки за защита и контрол на достъпа съобразно спецификата на водените регистри;

3. Осъществява контрол по спазване на изискванията по защита на регистрите;

4. Специфицира техническите ресурси, прилагани за обработване на личните данни;

5. Подпомага установяването на обстоятелства, свързани с нарушаване на защитата на регистрите;

6. В случай на установяване на нарушение на сигурността на личните данни, лицето по защита на личните данни уведомява в спешен порядък администратора на лични данни. Настъпилото събитие поражда задължение за администратора на лични данни в рамките на 72 часа от установяване на нарушението незабавно да уведоми КЗЛД за нарушаване сигурността на личните данни в детска градина/училище

7. Поддържа връзка с Комисията за защита на личните данни (КЗЛД) относно предприетите мерки и средства за защита на регистрите;

8. Контролира спазването на правата на потребителите във връзка с регистрите и програмно-техническите ресурси за тяхната обработка;

9. Периодично информира персонала по въпросите на защитата на личните данни;

10. Следи за спазване на организационните процедури за обработване на личните данни и провежда периодичен контрол за спазване на изискванията по защита на данните и при открити нередности взема мерки за тяхното отстраняване.

Чл. 25. (1) С цел недопускането на неправомерен достъп, както и всички други незаконни форми на обработване на личните данни, администраторът организира и предприема мерки, съобразени със съвременните технологични постижения и рисковете, свързани с естеството на данните, които трябва да бъдат защитени.

(2) Видове защита:

1. Физическа защита на личните данни представлява система от технически и организационни мерки за предотвратяване на нерегламентиран достъп до сгради, помещения и съоръжения, в които се обработват лични данни.

2. Персонална защита представлява система от организационни мерки спрямо физическите лица, които обработват лични данни по указание на администратора.

3. Документална защита представлява система от организационни мерки при обработването на лични данни на хартиен носител.

4. Защита на автоматизираните информационни системи и/или мрежи представлява система от технически и организационни мерки за защита от незаконни форми на обработване на личните данни.

5. Псевдонимизация чрез употребата на технически и организационни мерки.

Чл. 26 (1) Всяко лице, желаещо да внесе документ съдържащ лични данни, предоставя същия в деловодството на ПГХТБТ „Мария Кюри“

Лицето приемащо документа е задължено да запознае вносителя на документите с правата му на субект на лични данни, както и с Вътрешните правила за тяхната обработка. Преди приемането му, вносителят попълва съответна Декларация по образец предоставена му от лицето приемащо документите за деклариране на предоставените лични данни и основанието, на което те се предоставят и ще се ползват. Лицето, приемащо документите има право да изиска от субекта на лични данни документа, доказващ истинността на предоставените лични данни, а при наличие на предвидена в закона възможност, да снима копие от този документ и да го приложи към декларацията.

(2) Внесените документи с лични данни се докладват на Директора, който ги разпределя на лицата обработващи съответните лични данни.

(3) Лицата обработващи личните данни са задължени да предоставят личните данни в съответствие с разпореждането на Директора на Администратора.

(4) Лични данни се предоставят на трети лица само чрез Директора на Администратора.

(5) При предоставяне на личните данни за ползване то трети лица, те попълват декларация за задължението си да обработват личните данни съгласно Регламент 2016/679 и ЗЗЛД.

2. МЕРКИ ЗА ЗАЩИТА ПРИ ОБРАБОТВАНЕ НА ЛИЧНИТЕ ДАННИ

Чл. 27. (1) Правилата за защита при обработване на лични данни регламентират технически мерки, които:

1. Отхвърлят достъпа на неоторизирани лица до оборудването за обработка на данни – контрол на достъпа до оборудване;

2. Предотвратяват неоторизираното четене, копиране, промяна или унищожаване на информационни носители – контрол на информационните носители;

3. Предотвратяват неоторизираното добавяне, въвеждане, преглеждане, промяна или заличаване на съхранени лични данни – контрол по съхраняването;

4. Предотвратяват използването му от неоторизирани лица, използващи комуникационно оборудване за данни – контрол на потребителите;

5. Гарантират, че лицата, които са оторизирани да ползват система за автоматизирана обработка на данни, имат достъп само до данните, включени в обхвата на техния достъп – контрол на достъпа до данни;

6. Осигуряват възможността за проверка и установяване до кои органи са били или могат да бъдат изпратени или предоставени личните данни чрез използване на комуникационно оборудване за данни – контрол на комуникациите;

7. Осигуряват възможност за последваща проверка и установяване какви лични данни са въведени в системите за автоматизирана обработка на данни, кога и от кого са въведени данните – контрол на въвеждане;

8. Предотвратяват неоторизирано четене, копиране, промяна или изтриване на лични данни при трансфер на лични данни или превозване на носители на данни – контрол при транспортиране;

9. Осигуряване на възможност инсталираните системи да могат да се възстановят в случаи на прекъсване на функционирането – възстановяване;

10. Осигуряват правилното функциониране на системата, докладване на появата на грешки във функциите (надеждност) и гарантират, че съхранените данни не могат да бъдат повредени чрез неправилно функциониране на системата – интегритет.

Чл.28. (1) Служителят/ите, обработващ/и лични данни, взема/т мерки за гарантиране на надеждност при обработването, като осъществява/т технически и организационни мерки за защита на личните данни.

(2) При автоматичната обработка на лични данни се осъществяват технически мерки за защита срещу:

1. Неоторизирано четене, възпроизвеждане, промяна или премахване на носителя на данните;

2. Неоторизирано въвеждане, промяна или заличаване на съхранени лични данни;

3. Неоторизирано използване на системите за лични данни чрез средства за пренос на данни;

4. Неоторизиран достъп до лични данни.

Глава пета

ОЦЕНКА НА ВЪЗДЕЙСТВИЕТО ВЪРХУ ОБРАБОТВАНИТЕ ЛИЧНИ ДАННИ

Чл.29. (1). Оценката на въздействието е процес за определяне нивата на въздействие върху конкретно физическо лице или група физически лица в зависимост от характера на обработваните лични данни и броя на засегнатите физически лица при нарушаване на поверителността, цялостността или наличността на личните данни.

(2) Оценката на въздействието се извършва периодично на всеки две години или при промяна на характера на обработваните лични данни и броя на засегнатите физически лица.

Чл.30. При оценката на въздействието администраторът отчита характера на обработваните лични данни, както следва:

1. Систематизиране и оценка на лични аспекти, свързани с дадено физическо лице (профилиране), за анализиране или прогнозиране, по-специално на неговото икономическо положение, местоположение, лични предпочитания, надеждност или поведение и др.

2. Данни, които разкриват расов или етнически произход, политически, религиозни или философски убеждения, членство в политически партии или организации, сдружения с религиозни, философски, политически или синдикални цели, или данни, които се отнасят до здравето, сексуалния живот или до човешкия геном;

3. Лични данни чрез създаване на видеозапис от видеонаблюдение на публично достъпни райони;

4. Лични данни в широкомащабни регистри на лични данни;

5. Данни, чието обработване съгласно решение на Комисията за защита на личните данни застрашава правата и законните интереси на физическите лица.

НИВА НА ВЪЗДЕЙСТВИЕ

Чл.31. Определят се следните нива на въздействие

1. „Изключително високо” – в случаите, когато неправомерното обработване на лични данни би могло да доведе до възникване на значителни вреди или кражба на самоличност на особено голяма група физически лица или трайни здравословни увреждания или смърт на група физически лица;

2. „Високо” – в случаите, когато неправомерното обработване на лични данни би могло да доведе до възникване на значителни вреди или кражба на самоличност на голяма група физически лица или лица, заемащи висши държавни длъжности, или трайни здравословни увреждания или смърт на отделно физическо лице;

3. „Средно” – в случаите, когато неправомерното обработване на лични данни би могло да създаде опасност от засягане на интереси, разкриващи расов или етнически произход, политически, религиозни или философски убеждения, членство в политически партии или организации, сдружения с религиозни, философски, политически или синдикални цели, здравословното състояние, сексуалния живот или човешкия геном на отделно физическо лице или група физически лица;

4. „Ниско” – в случаите, когато неправомерното обработване на лични данни би застрашило неприкосновеността на личността и личния живот на отделно физическо лице или група физически лица.

Чл.32. (1) Администраторът извършва оценка на въздействие за всички поддържани регистри .

(2) Всеки отделен регистър се оценява по критериите поверителност, цялостност и наличност.

(3) Най-високото ниво на въздействие, определено по всеки от критериите по ал. 2, определя нивото на въздействие на съответния регистър.

Чл.33. В зависимост от нивото на въздействие се определя и съответно ниво на защита.

Чл.34. (1) Нивата на защита са ниско, средно, високо и изключително високо.

(2) Нивата на защита са, както следва:

1. При ниско ниво на въздействие – ниско ниво на защита;
2. При средно ниво на въздействие – средно ниво на защита;
3. При високо ниво на въздействие – високо ниво на защита;
4. При изключително високо ниво на въздействие – изключително високо ниво на защита.

Глава шеста

ПРОЦЕДУРИ ЗА ДОКЛАДВАНЕ И УПРАВЛЕНИЕ ПРИ ИНЦИДЕНТИ

Чл.35. (1) При възникване и установяване на инцидент и/или нерегламентиран достъп, свързан с нарушаване защитата или загуба на лични данни, незабавно се докладва на лицето по защита на личните данни в ПГХТБТ „Мария Кюри“

- (2) За инцидентите се води регистър, в който задължително се вписват предполагаемото време или период на възникване, времето на установяване, времето на докладване и името на служителя, извършил доклада.
- (3) След анализ от лицето по защита на личните данни, в регистъра се записват последствията от инцидента и мерките, които са предприети за отстраняването им.
- (4) В случаите на необходимост от възстановяване на данни, процедурата се изпълнява след писменото разрешение на лицето по защита на личните данни, като това се отразява в регистър по архивиране и възстановяване на данни.
- (5) В случаите на компрометиране на парола, тя се подменя с нова, като събитието се отразява в регистъра за инциденти.

Глава осма

ОТГОВОРНОСТ

Чл.36. За неизпълнение на задълженията, вменени на съответните оправомощени лица по тези Правила, по ЗЗЛД и по Регламент (ЕС) 2016/679, се налагат дисциплинарни наказания по Кодекса на труда, а когато неизпълнението на съответното задължение е констатирано и установено от надлежен орган – предвиденото в ЗЗЛД административно наказание, ако такава отговорност се предвижда по закон.

Чл.37. (1) За вреди, причинени в резултат на незаконосъобразно обработване на лични данни от служители в ПГХТБТ „Мария Кюри“, засегнатите лица могат да търсят отговорност от виновните лица по реда на общото гражданско законодателство или наказателна отговорност, ако извършеното представлява престъпление.

(2) Ако в резултат на незаконосъобразно обработване на лични данни, включително незаконното им разкриване или разпространение, са причинени щети на администратора на лични данни, на виновните лица се търси имуществена отговорност по Кодекса на труда .

Настоящите правила са утвърдени със Заповед № РД-08-236/25.04.2023г.

За всички неуредени случаи се прилагат разпоредбите на Регламент 2016/679, ЗЗЛД и разпоредженията на Директора на образователната институция