



**ПРОФИЛИРАНА ГИМНАЗИЯ С ИНТЕНЗИВНО ИЗУЧАВАНЕ НА
РУМЪНСКИ ЕЗИК „МИХАЙ ЕМИНЕСКУ“**

гр. София, ул. „Стара Планина“ № 13, 0877004456,

e-mail: eminesku@abv.bg

УТВЪРЖДАВАМ:

Виолета Йосифова,
Директор на ПГИИРЕ



**ВЪТРЕШНИ ПРАВИЛА
ЗА МЕРКИТЕ И СРЕДСТВАТА ЗА ОБРАБОТВАНЕ И
ЗАЩИТА НА ЛИЧНИ ДАННИ**

на ПГИИРЕ „Михай Еминеску“

СОФИЯ

Чл. 1. (1) С тези вътрешни правила се уреждат редът и условията за набиране, обработване, актуализация, съхраняване, предоставяне, трансфер и унищожаване на личните данни, както и мерките и средствата за тяхната защита.

(2) Настоящите правила се издават на основание Регламент (ЕС) 2016/679 (Общ регламент относно защитата на данните) и Закона за защита на личните данни (ЗЗЛД).

(3) Правилата се утвърждават, допълват, изменят и отменят от Директора на ПГИИРЕ „Михай Еминеску“ – администратор на лични данни.

(4) Администраторът осигурява упражняването на правата на субектите на лични данни и предоставя достъп до личните данни съобразно условията и ограниченията, предвидени в Регламент (ЕС) 2016/679 и ЗЗЛД.

ЦЕЛИ И ОБХВАТ НА ПРАВИЛАТА

Чл. 2. Настоящите Правила имат за цел да регламентират:

(1) механизмите за набиране, обработване, актуализация, съхраняване, предоставяне, трансфер и унищожаване на личните данни;

(2) задълженията на Администратора, лицата обработващи лични данни, длъжностното лице по защита на лични данни и тяхната отговорност при неизпълнение на тези задължения;

(3) правилата за разпределение на личните данни и групирането им в регистри и Правилата за работа с личните данни;

(4) необходимите технически и организационни мерки за защита личните данни от неправомерно обработване (случайно или незаконно разрушаване, случайна загуба или промяна, незаконно разкриване или достъп, нерегламентирано изменение или разпространение, както и от всички други незаконни форми на обработване на лични данни).

Чл. 3. Правилата са задължителни за всички лица имащи достъп до личните данни, обработвани за нуждите на администратора.

ПРЕДНАЗНАЧЕНИЕ И ВИДОВЕ РЕГИСТРИ

Чл. 4. (1) В изпълнение на дейностите си ПГИИРЕ „Михай Еминеску“ поддържа следните видове регистри, съдържащи лични данни:

1. Регистър „Служители“.

2. Регистър „Доставчици“.

3. Регистър „Учащи“.

4. Регистър „Родители“.

5. Регистър „Лични лекари“.

6. Регистър „Пропускателен режим“.

7. Регистър „Видеонаблюдение“.

4.1. РЕГИСТЪР „СЛУЖИТЕЛИ“

4.1.1. Общо описание на регистъра

4.1.1.1. Цели на обработване на лични данни: администриране на трудовите и гражданските правоотношения в ПГИИРЕ, определяне и изплащане на възнагражденията, изпълнение на задълженията по трудовото и осигурителното законодателство и осигуряване на здравословни и безопасни условия на труд.

4.1.1.2. Нормативно основание: Кодекс на труда, Кодекс за социално осигуряване, Закон за данъците върху доходите на физическите лица, Закон за здравословни и безопасни условия на труд, Наредба № 8 от 11.08.2016 г. за информацията и документите за системата на предучилищното и училищното образование и други приложими нормативни актове.

4.1.1.3. Категории физически лица, за които се обработват данните: лица, работещи по трудово правоотношение, лица по граждански договори и кандидати за работа в ПГИИРЕ.

4.1.1.4. Категории лични данни:

- физическа идентичност – трите имена, ЕГН/личен идентификатор, адрес, данни от документ за самоличност, месторождение, телефон;
- данни за здравословното състояние – медицинска документация, когато събирането и обработването ѝ е необходимо за изпълнение на нормативно установени задължения;
- образование и професионална квалификация – образование, допълнителна квалификация, степени, звания, данни от документи за придобита квалификация;
- трудова и професионална идентичност – данни за трудова дейност, професионален опит, професионална автобиография и данни, свързани с трудовото правоотношение;
- семейно положение – когато данните са необходими за изпълнение на нормативно установени задължения;
- банкови сметки, данни за изплащане на трудови възнаграждения и други дължими плащания;
- данни от свидетелства за съдимост или други документи, удостоверяващи наличието или липсата на обстоятелства, когато това се изисква по закон.

4.1.1.5. Източници, от които се събират данните:

- от физическите лица, за които се отнасят данните, когато това е необходимо за изпълнение на трудовото или гражданското правоотношение или на нормативно установени задължения;
- от публични регистри и компетентни институции, когато това е предвидено в закон или е необходимо за изпълнение на нормативно установени задължения;
- от други законово допустими източници, когато това е необходимо за изпълнение на дейностите на ПГИИРЕ.

4.1.2. Технологично описание на регистъра

4.1.2.1. Носители на данни

Данните в регистър „Служители“ в ПГИИРЕ се събират и обработват на хартиен носител и в информационни системи и софтуерни продукти, използвани от ПГИИРЕ, в съответствие с приложимите нормативни изисквания.

Хартиените носители на лични данни се съхраняват в кадрови досиета в шкафове с ограничен достъп и при необходимост – с ключалка. Автоматизираното обработване на данните се осъществява на компютри и други технически средства със защитен достъп чрез потребителско име и парола и други приложими технически и организационни мерки.

Личните данни се поддържат във вида и формата, които позволяват идентифициране самоличността на физическите лица.

4.1.2.2. Технология на обработване

Данните в регистър „Служители“ се използват за изготвяне и съхраняване на трудови и граждански договори, допълнителни споразумения, ведомости за заплати, документи, удостоверяващи трудов стаж и професионален опит, служебни бележки, справки, удостоверения и други документи, свързани с изпълнение на задълженията на ПГИИРЕ.

Обработката на данните се осъществява както на хартиен носител, така и в електронен вид. Личните данни се съхраняват в определени за целта служебни помещения и информационни системи с ограничен достъп.

4.1.2.3. Срок на съхранение

Данните в регистър „Служители“ се съхраняват, както следва:

- досиетата на персонала в цялост се съхраняват 5(пет) години след прекратяване на трудовото правоотношение;
- документи свързани с ведомости за заплати се съхраняват 50(петдесет) години;

4.1.2.4. Предоставени услуги

ПГИИРЕ не обработва личните данни от регистър „Служители“ за други цели, извън посочените в т. 4.1.1.1, освен когато обработването е необходимо за изпълнение на нормативно установено задължение или е допустимо на друго законово основание.

4.1.3. Длъжности, свързани с обработването и защитата на лични данни от регистър „Служители“, права и задължения

4.1.3.1. Данните в регистър „Служители“ се събират, обработват и съхраняват при спазване на принципа „Необходимост да се знае“ от лица – служители на ПГИИРЕ, както следва:

- секретар;
- счетоводител;
- директор на ПГИИРЕ.

Достъпът до личните данни се предоставя съобразно служебните задължения на съответните лица и предоставените им права за достъп.

4.2. РЕГИСТЪР „ДОСТАВЧИЦИ“

4.2.1. Общо описание на регистъра

4.2.1.1. Цели на обработване на лични данни: сключване и изпълнение на договори с доставчици с цел обезпечаване материално и технически дейността на ПГИИРЕ, както и извършване на плащания за предоставените стоки и услуги.

4.2.1.2. Нормативно основание: Закон за обществените поръчки, Правилник за прилагане на Закона за обществените поръчки, Закон за задълженията и договорите, приложимото данъчно и счетоводно законодателство и други приложими нормативни актове.

4.2.1.3. Категории физически лица, за които се обработват данните: физически лица – кандидати и участници в обществени поръчки и конкурси, представители и лица за контакт на доставчици и изпълнители, както и физически лица – изпълнители по договори.

4.2.1.4. Категории лични данни:

- физическа идентичност – трите имена, ЕГН/личен идентификатор, адрес, телефон, електронен адрес и данни от документ за самоличност, когато това е необходимо;
- професионална идентичност – длъжност, професионален опит, образование и квалификация, когато са относими към конкретната процедура или договор;
- данни за банкови сметки и плащания, когато са необходими за изпълнение на договорните и финансовите задължения;
- данни от свидетелства за съдимост или други документи, удостоверяващи наличие или липса на определени обстоятелства, когато това се изисква по закон.

4.2.1.5. Източници, от които се събират данните:

- от физическите лица, за които се отнасят данните;
- от юридически лица и еднолични търговци, когато данните са предоставени за техни представители, пълномощници или лица за контакт;
- от публични регистри и други официални източници, когато това е допустимо и необходимо за изпълнение на дейността.

4.2.2. Технологично описание на регистъра

4.2.2.1. Носители на данни

Данните в регистър „Доставчици“ се събират, обработват и съхраняват на хартиен носител и в електронен вид на компютри и други технически средства с ограничен достъп.

Хартиените носители на лични данни се съхраняват в определени за целта служебни помещения и шкафови с ограничен достъп. Помещенията, в които се обработва и съхранява регистърът, са с контролиран и ограничен достъп.

4.2.2.2. Технология на обработване

Данните в регистър „Доставчици“ се използват при изготвяне и съхраняване на документи, свързани с избор на изпълнители за доставки и услуги, граждански договори, договори за доставки и услуги и други договори, свързани с обезпечаване дейността на ПГИИРЕ.

Обработката на данните се осъществява на хартиен носител, а при необходимост и в електронен вид.

4.2.2.3. Срок на съхранение

Данните в регистър „Доставчици“ се съхраняват за сроковете, определени в приложимото законодателство, като отделните документи се съхраняват за съответния нормативно установен срок.

Документите, за които нормативната уредба предвижда по-дълъг срок на съхранение, се съхраняват за съответния срок.

4.2.2.4. Предоставени услуги

ПГИИРЕ не обработва личните данни от регистър „Доставчици“ за други цели, извън посочените в т. 4.2.1.1, освен когато обработването е необходимо за изпълнение на нормативно установено задължение или е допустимо на друго законово основание.

4.2.3. Длъжности, свързани с обработването и защитата на лични данни от регистър „Доставчици“, права и задължения

4.2.3.1. Данните в регистър „Доставчици“ се събират, обработват и съхраняват при спазване на принципа „Необходимост да се знае“ от лица – служители на ПГИИРЕ, както следва:

- секретар;
- домакин;
- счетоводител;
- директор на ПГИИРЕ.

При провеждане на обществени поръчки в обработването на лични данни могат да участват лица – служители, определени със заповед на директора на ПГИИРЕ, в която се посочват конкретните им задължения и права за достъп до лични данни.

Правата и задълженията на служителите, работещи с лични данни, са регламентирани в длъжностните им характеристики и/или в заповедите на директора.

4.3. РЕГИСТЪР „УЧАЩИ“

4.3.1. Общо описание на регистъра:

4.3.1.1. Цели на обработване на лични данни: изпълнение на нормативно възложени задължения във връзка с обучението, възпитанието и образованието на учениците, организацията на учебния процес и воденето на необходимата документация.

4.3.1.2. Нормативно основание: Закон за предучилищното и училищното образование и произтичащите от него подзаконови нормативни актове, Наредба № 8 от 11.08.2016 г. за информацията и документите за системата на предучилищното и училищното образование, Правилник за дейността на ПГИИРЕ „Михай Еминеску“ и други приложими нормативни актове.

4.3.1.3. Категории физически лица, за които се обработват данните:

- ученици в ПГИИРЕ;

– кандидати за прием в ПГИИРЕ.

4.3.1.4. Категории лични данни:

– физическа идентичност – трите имена, ЕГН/личен идентификатор, адрес, месторождение, телефон, дата и година на раждане и други идентификационни данни, когато са нормативно определени;

– данни за здравословното състояние – данни за здравословното състояние, личен лекар и медицинска документация от ЛКК, ТЕЛК, НЕЛК и други компетентни медицински органи, когато събирането и обработването им е нормативно предвидено;

– данни за образование и обучение – данни за образование, резултати от обучението, отсъствия, участие в образователния процес и други данни, свързани с обучението;

– семейни данни – данни за родители, настойници или други законни представители и данни за семейното положение, когато са необходими за изпълнение на нормативно установени задължения.

4.3.1.5. Източници, от които се събират данните:

– от физическите лица, за които се отнасят данните, когато това е приложимо;

– от родителите, настойниците или другите законни представители;

– от компетентни институции и публични регистри, когато това е предвидено в нормативен акт;

– чрез информационни системи и други законово установени източници на информация.

4.3.2. Технологично описание на регистъра

4.3.2.1. Носители на данни

Данните в регистър „Учащи“ се събират и обработват на хартиен носител и в електронен вид чрез Националната електронна информационна система за предучилищното и училищното образование (НЕИСПУО) и електронния дневник „Школо“, съгласно приложимите нормативни изисквания.

4.3.2.2. Технология на обработване

Личните данни в регистър „Учащи“ се обработват на хартиен носител и в електронен вид при спазване на принципа „Необходимост да се знае“.

Личните данни на учениците се съхраняват в определени за целта служебни помещения и се предоставят на учители и други служители само доколкото това е необходимо за изпълнение на служебните им задължения и в съответствие с предоставените им права за достъп. Част от информацията се съдържа и в документацията на паралелките и в дневниците.

Данните на учащите се въвеждат и обработват в НЕИСПУО и в електронния дневник „Школо“ съобразно нормативните изисквания и предоставените права за достъп.

Достъпът до електронните системи се осъществява чрез индивидуални потребителски профили и пароли, съобразно определените права за достъп.

Помещенията, в които се обработва и съхранява регистърът, са с ограничен достъп и при необходимост са оборудвани със заключващи се шкафове.

4.3.2.3. Срок на съхранение

Личните данни в регистър „Учащи“ се съхраняват за сроковете, определени в приложимите нормативни актове, включително в нормативната уредба относно информацията и документите за системата на предучилищното и училищното образование.

4.3.2.4. Предоставени услуги

ПГИИРЕ не обработва личните данни от регистър „Учащи“ за други цели, извън посочените в т. 4.3.1.1, освен когато обработването е необходимо за изпълнение на нормативно установено задължение или е допустимо на друго законово основание.

4.3.3. Длъжности, свързани с обработването и защитата на лични данни от регистър „Учащи“

4.3.3.1. Данните в регистър „Учащи“ се събират, обработват и съхраняват при спазване на принципа „Необходимост да се знае“ от лица – служители на ПГИИРЕ, както следва:

- секретар;
- учители;
- домакин, когато е необходимо за изпълнение на служебните му задължения;
- директор.

Правата и задълженията на служителите, работещи с лични данни, са регламентирани в длъжностните им характеристики и/или в заповедите на директора.

ПГИИРЕ обработва само лични данни, които са необходими и нормативно определени за изпълнение на съответните дейности и задължения, при спазване на принципите за законосъобразност, добросъвестност, прозрачност и минимизиране на данните.

4.4. РЕГИСТЪР „РОДИТЕЛИ И НАСТОЙНИЦИ“

4.4.1. Общо описание на регистъра

4.4.1.1. Цели на обработването:

Изпълнение на нормативно установените задължения на училището във връзка с обучението, възпитанието и образованието на учениците; осигуряване на необходимата комуникация с родителите, настойниците, попечителите и другите законни представители; упражняване и изпълнение на правата и задълженията на родителите и законните представители; както и определяне и отпускане на стипендии и други форми на финансова подкрепа, когато това е предвидено в нормативните актове.

4.4.1.2. Нормативно основание:

Регламент (ЕС) 2016/679, Закон за защита на личните данни, Закон за предучилищното и училищното образование и подзаконовите нормативни актове по прилагането му, Правилникът за дейността на ПГИИРЕ „Михай Еминеску“, нормативните актове,

регламентиращи отпускането на стипендии и други форми на финансова подкрепа, както и други приложими нормативни актове.

4.4.1.3. Категории физически лица:

- родители на ученици;
- настойници и попечители;
- други законни представители на учениците, когато е приложимо.

4.4.1.4. Категории лични данни:

- физическа идентичност – трите имена, ЕГН/личен идентификатор, адрес, телефон, електронен адрес и други данни за контакт, когато са необходими;
- данни за връзката с ученика – данни за качеството на родител, настойник, попечител или друг законен представител;
- данни за семейното положение, когато са необходими за изпълнение на нормативно установени задължения;
- данни за доходи и други обстоятелства, свързани с материалното положение на семейството, когато са необходими за определяне и отпускане на стипендии и други форми на финансова подкрепа, предвидени в нормативните актове;
- данни за банкови сметки, когато са необходими за изплащане на стипендии или други дължими плащания.

4.4.1.5. Източници на личните данни:

Личните данни се получават от самите физически лица, от учениците, когато това е приложимо, от компетентни държавни и общински органи и институции, публични регистри и други законосъобразни източници, когато това е необходимо за изпълнение на нормативно установени задължения.

4.4.2. Начин на водене и съхраняване

4.4.2.1. Данните се обработват на хартиен и електронен носител, включително чрез НЕИСПУО и електронния дневник „Школо“, когато съответното обработване е предвидено и необходимо за изпълнение на задълженията на училището.

4.4.2.2. Достъпът до личните данни се предоставя само на лица, за които същият е необходим за изпълнение на служебните им задължения. Данни за родителите и законните представители могат да бъдат предоставяни на педагогическия и непедагогическия персонал само в необходимия обем и за конкретна служебна цел. Документите на хартиен носител се съхраняват в определени за целта служебни помещения и/или заключени шкафове. Електронните данни се обработват чрез определени информационни системи при използване на индивидуални профили, пароли и други подходящи технически и организационни мерки.

4.4.2.3. Данните в регистър „Родители и настойници“ се предоставят и съхраняват на хартиен носител и електронен носител, съгласно Наредба № 8 от 11.08.2016 г. за информацията и документите за системата на предучилищното и училищното образование.

4.4.2.4. Личните данни не се използват за цели, несъвместими с целите, за които са събрани, освен когато обработването е необходимо за изпълнение на нормативно установено задължение или е налице друго приложимо правно основание.

4.4.3. Достъп до личните данни

4.4.3.1. Достъп до личните данни в регистъра имат директорът, педагогическите специалисти и други служители, на които достъпът е необходим за изпълнение на служебните им задължения, в рамките на предоставените им права за достъп. Правата и задълженията на лицата се определят с длъжностните характеристики, заповеди на директора и други вътрешни актове на училището.

При обработването на данните училището събира и използва само данните, които са необходими за конкретната цел и са предвидени в приложимите нормативни актове, като се спазват принципите на законосъобразност, добросъвестност, прозрачност и свеждане на данните до минимум.

4.5. РЕГИСТЪР „ЛИЧНИ ЛЕКАРИ“

4.5.1. Общо описание на регистъра

4.5.1.1. Цели на обработване на лични данни: за изпълнение на нормативно възложени задължения свързани със здравословното състояние на персонала и учащите се.

4.5.1.2. Нормативно основание: Закона за предучилищното и училищното образование и произтичащите от него подзаконови актове.

4.5.1.3. Категории физически лица, за които се обработват данните:

– физически лица – лекари;

4.5.1.4. Категории лични данни:

– физическа идентичност – трите имена, адрес на практиката, телефон.

4.5.1.5. Източници, от които се събират данните:

– физически лица – родители или настойници на учащи в ПГИИРЕ, които предоставят данни за личните лекари на учащите се в ПГИИРЕ.

4.5.2. Технологично описание на регистъра

4.5.2.1. Носители на данни

Данните в регистър „Лични лекари“ се предоставят и съхраняват на хартиен носител и електронен носител, съгласно Наредба № 8 от 11.08.2016 г. за информацията и документите за системата на предучилищното и училищното образование.

4.5.2.2. Технология на обработване

Данните в регистър „Лични лекари“ се обработват на хартиен носител в помещения с ограничен достъп и на електронен носител, съгласно Наредба № 8 от 11.08.2016 г. за информацията и документите за системата на предучилищното и училищното образование. Част от информацията се предоставя на учителите /чрез дневниците на паралелките/ за изпълнение на служебните им задължения и за евентуална реакция при нужда. Помещенията

са оборудвани със заключващи се шкафове, а достъпът до компютрите се осъществява чрез потребителско име и парола. Компютрите са свързани в локална мрежа или са извън нея.

4.5.2.3. Срок на съхранение

Данните в регистър „Лични лекари“ се съхраняват съгласно сроковете, посочени в Наредба № 8 от 11.08.2016 г. за информацията и документите за системата на предучилищното и училищното образование.

4.5.2.4. Предоставени услуги

ПГИИРЕ не обработва личните данни от регистър „Лични лекари“ за други цели, извън посочените в т. 4.5.1.1.

4.5.3. Длъжности, свързани с обработването и защитата на лични данни от регистър „ЛИЧНИ ЛЕКАРИ“, права и задължения

4.5.3.1. Данните в регистър „ЛИЧНИ ЛЕКАРИ“ се събират, обработват и съхраняват при спазване на принципа „Необходимост да се знае“ от лица – служители на ПГИИРЕ:

- учители;
- медицинска сестра;
- директор.

4.6. РЕГИСТЪР „ПРОПУСКАТЕЛЕН РЕЖИМ“

4.6.1. Общо описание на регистъра

4.6.1.1. Цели на обработване на личните данни: осигуряване на пропускателния режим и контрол на достъпа до сградата на ПГИИРЕ, както и опазване на сигурността в сградата.

4.6.1.2. Нормативно основание: Закон за частната охранителна дейност, Правилник за пропускателния режим в ПГИИРЕ и други приложими нормативни и вътрешни актове.

4.6.1.3. Категории физически лица, за които се обработват данните: учители, служители, ученици, родители, граждани и изпълнители по договори, външни посетители.

4.6.1.4. Категории лични данни:

- физическа идентичност – име, презиме, фамилия.

4.6.1.5. Източници, от които се събират данните:

- от физическите лица, за които се отнасят данните.

4.6.2. Технологично описание на регистъра

4.6.2.1. Носители на данни

Данните в регистър „Пропускателен режим“ се събират, обработват и съхраняват на хартиен носител.

Мястото, на което се събират, обработват и съхраняват данните, е с ограничен достъп.

4.6.2.2. Технология на обработване

Данните се предоставят от физическите лица – посетители, външни изпълнители и други лица, за които това е необходимо съгласно установения в училището пропускателен режим, при влизане в сградата на ПГИИРЕ.

4.6.2.3. Срок на съхранение

Данните в регистър „Пропускателен режим“ се съхраняват за срок от 1(една) година.

4.6.2.4. Предоставени услуги

ПГИИРЕ не обработва личните данни от регистър „Пропускателен режим“ за други цели, извън посочените в т. 4.6.1.1.

4.6.3.1. Данните от регистър „Пропускателен режим“ се събират, обработват и съхраняват при спазване на принципа „Необходимост да се знае“ от дежурния портиер и от други определени със заповед на директора лица.

4.7. РЕГИСТЪР „ВИДЕОНАБЛЮДЕНИЕ“

4.7.1. Общо описание на регистъра:

4.7.1.1. Цели: Осигуряване на сигурността на учениците, педагогическите специалисти, служителите и посетителите на територията на ПГИИРЕ „Михай Еминеску“, защита на имуществото, както и предотвратяване и установяване на инциденти и нарушения.

4.7.1.2. Нормативно основание: Регламент (ЕС) 2016/679 (Общ регламент относно защитата на данните – GDPR), Закон за защита на личните данни и приложимото национално законодателство.

4.7.1.3. Категории физически лица: Педагогически специалисти, служители, ученици, родители, граждани, изпълнители по договори, външни посетители и други лица, намиращи се на територията на ПГИИРЕ „Михай Еминеску“.

4.7.1.4. Категории лични данни: Визуална информация и изображения на физически лица, попадащи в обхвата на видеонаблюдението.

4.7.1.5. Източник на данните: Данните се получават чрез системата за видеонаблюдение, функционираща на територията на ПГИИРЕ „Михай Еминеску“.

4.7.2. Технически характеристики и обработване

4.7.2.1. Данните се събират и обработват чрез система за видеонаблюдение и се съхраняват в електронен вид в системата за видеозапис. Камери са разположени на входа, в коридорите и в учебните кабинети на ПГИИРЕ „Михай Еминеску“.

4.7.2.2. Видеонаблюдението се извършва непрекъснато. Достъпът до системата и до записите се предоставя само на лица, определени със заповед на директора, съобразно служебните им задължения и предоставените им права на достъп.

4.7.2.3. Записите се съхраняват за срок, определен от училището съобразно целите на видеонаблюдението, необходимостта от съхраняването им и приложимите изисквания за защита на личните данни. След изтичане на определения срок записите се изтриват или се презаписват. Когато е необходимо във връзка с конкретен инцидент, проверка, сигнал или

производство, съответните записи могат да бъдат съхранявани за по-дълъг срок, доколкото това е необходимо и допустимо по закон.

4.7.2.4. Данните от видеонаблюдението не се използват за цели, несъвместими с целите, за които са събрани. Записи могат да бъдат предоставяни на компетентни държавни органи или на други оправомощени лица само при наличие на правно основание и при спазване на изискванията за защита на личните данни.

4.7.3. Достъп до записите

Достъпът до системата за видеонаблюдение и до записите се предоставя съобразно принципа „необходимост да се знае“ и само на лица, на които е предоставен достъп със заповед на директора, съобразно служебните им задължения.

4.7.4. Информирание на лицата

На видими места са поставени информационни обозначения, чрез които лицата се уведомяват за извършваното видеонаблюдение.

4.7.5. Ограничения

Не се извършва видеонаблюдение в санитарни помещения, съблекални и други места, в които наблюдението би засегнало неоправдано личната неприкосновеност и правото на личен живот на лицата.

4.7.6. Мерки за защита

Прилагат се подходящи технически и организационни мерки за защита на записите и системата за видеонаблюдение срещу неправомерен достъп, изменение, копиране, разпространение, загуба или унищожаване.

4.7.7. Конфиденциалност

Лицата, получили достъп до системата и записите от видеонаблюдението, са длъжни да спазват изискванията за поверителност и да не предоставят или разкриват информация на неупълномощени лица.

Форми на водене на регистрите

Чл. 5. (1) Формите на водене на регистрите са на хартиен и технически носител.

1. Водене на регистър на хартиен носител:

1.1. Форма на организация и съхраняване на личните данни – писмена (документална);

1.2. Местонахождение на картотечните шкафове: канцеларията на секретаря, кабинета на директора и кабинета на заместник-директора;

(2) Форма за предоставяне на данните от физическите лица – хартиена. Личните данни се предоставят на администратора на лични данни или на определени от него лица, когато това е необходимо за изпълнение на нормативно установени или служебни задължения.

1. Достъп до личните данни имат само определените със заповед на директора лица, доколкото това е необходимо за изпълнение на служебните им задължения.

(3) Водене на регистър на технически носител:

1. Форма на организация и съхраняване на личните данни – личните данни се съхраняват на технически носители и в информационни системи, като достъпът до тях се защитава чрез подходящи технически и организационни мерки, включително пароли, когато е приложимо;
2. Местонахождение на компютрите – в канцелариите и служебните кабинети на училището;
3. Достъп до личните данни и защита – достъп до електронни файлове, информационни системи и други технически средства, съдържащи лични данни, имат само определените със заповед на директора лица, съобразно служебните им задължения и предоставените им права на достъп. Достъпът се осъществява чрез подходящи технически и организационни мерки за защита на личните данни.
4. Видеонаблюдението се осъществява чрез система за видеонаблюдение, като видеозаписите се съхраняват на технически носител в системата за видеозапис. Достъп до системата и до съхраняваните видеозаписи имат само лицата, определени със заповед на директора.
5. Достъпът до системата за видеонаблюдение се осъществява при прилагане на подходящи технически и организационни мерки за защита на личните данни и записите от неправомерен достъп, копиране, изменение, разпространение, загуба или унищожаване.

Групи данни в регистрите

Чл. 6. (1) В зависимост от нормативното основание за събирането и предназначението им в регистрите се набират, обработват и съхраняват лични данни относно:

1. физическата идентичност на лицата – имена, ЕГН/личен идентификатор, данни от документ за самоличност, адрес, дата и място на раждане, телефони и други данни за контакт, когато са необходими;
2. семейна и роднинска принадлежност – данни за семейно положение, родствени връзки и данни за членове на семейството, когато са необходими за изпълнение на нормативно установени задължения;
3. образование и професионална квалификация – данни за образование, дипломи, квалификации, специалности и други данни, необходими за изпълнение на нормативно установени или служебни задължения;
4. трудова и служебна дейност – данни за трудови и други правоотношения, професионална биография, длъжност, трудов стаж, осигурителен стаж, осигурителен доход, основание за осигуряване и други данни, свързани с трудовата и служебната дейност;
5. здравни данни – данни относно здравословното състояние, медицински документи, диагнози и заключения на компетентни медицински органи, когато обработването им е предвидено в закон или е необходимо за изпълнение на нормативно установени задължения;
6. финансови и други лични данни – данни за трудови възнаграждения, парични обезщетения, банкови сметки и други финансови данни, когато са необходими за изпълнение на нормативно установени задължения, както и други категории лични данни, когато обработването им е предвидено в закон или е необходимо за изпълнение на дейността на училището.

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

Задължения на лицата, отговарящи за водене и съхраняване на данните в регистрите

Чл. 7. Лицата, определени със заповед на директора и/или на които е предоставен достъп до лични данни във връзка със служебните им задължения, са длъжни:

- да обработват личните данни само за определени и законосъобразни цели и в рамките на предоставените им права на достъп;
- да събират и обработват само необходимите за съответната дейност лични данни;
- да поддържат личните данни актуални и да предприемат необходимите действия за коригиране на неточни или непълни данни;
- да съхраняват личните данни по начин, който осигурява защита срещу неправомерен достъп, загуба, унищожаване, изменение или разкриване;
- да не предоставят лични данни на неупълномощени лица;
- да спазват изискванията за поверителност и сигурност на личните данни;
- при установяване на нарушение или риск за сигурността на личните данни да уведомят директора и определеното длъжностно лице по защита на данните, когато такова е определено.

Периодично архивиране

Чл. 8. . Архивирането на личните данни се извършва периодично, когато това е необходимо за изпълнение на нормативно установени изисквания и за осигуряване на съхраняването и възстановяването на необходимата информация. Архивирането се извършва от определени със заповед на директора лица или от лица, на които е предоставен съответният служебен достъп.

Чл. 9. Контролът върху дейностите по обработка на лични данни се осъществява от директора.

Актуализация на лични данни

Чл. 10. (1) Актуализация на лични данни представлява допълнение или изменение на съществуваща информация в училището. Актуализация на лични данни се извършва:

1. по искане на лицето, за което се отнасят личните данни, когато е установена неточност или непълнота в тях, като при необходимост искането се подкрепя с подходящи документи;
2. по инициатива на определено със заповед на директора лице или друго лице, на което е предоставен съответният служебен достъп, при наличие на информация или документ, даващи основание за актуализация;
3. при установена грешка или неточност при обработването на личните данни от страна на ПГИИРЕ „Михай Еминеску“.

(2) При актуализация на лични данни в досието на съответното лице се отразяват регистрационния номер на документа, източник на данните за актуализацията, дата на актуализацията. Актуализацията се извършва от лицето, обработващо личните данни.

ДОСТЪП ДО ЛИЧНИ ДАННИ

ОСИГУРЯВАНЕ НА ДОСТЪП НА ЛИЦАТА ДО ЛИЧНИТЕ ИМ ДАННИ

Чл. 11. (1) Всяко физическо лице има право на достъп до отнасящите се до него лични данни, обработвани от администратора, при условията и по реда на приложимото законодателство.

(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 до 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, както и за срока, за който се предвижда да бъдат съхранявани данните, или ако това е невъзможно – критериите за определяне на този срок, 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. 12. (1) Правото на достъп се осъществява с писмено заявление до администратора на лични данни. Заявлението може да бъде подадено и по електронен път.

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

Чл. 13. (1) Заявлението по чл. 12 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 заявлението от упълномощено лице към същото се прилага и нотариално завереното пълномощно.

(3) При получаване на заявлението то се регистрира в деловодната система на училището.

Чл. 14. (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 заявителя 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 би довела до необосновано увеличаване на разходите по предоставянето ѝ или технически затруднения.

Чл. 15. (1) Администраторът на лични данни разглежда заявлението и предприема необходимите действия без ненужно забавяне и във всички случаи не по-късно от един месец от получаването му.

(2) При необходимост, предвид сложността и броя на исканията, срокът по ал. 1 може да бъде удължен с до два месеца. Администраторът уведомява заявителя за удължаването в рамките на един месец от получаване на заявлението, като посочва причините за забавянето.

(3) С решението си администраторът предоставя пълна или частична информация на заявителя или мотивирано отказва предоставянето ѝ, когато са налице законови основания за това.

Чл. 16. Право на достъп до данните в поддържаните от администратора регистри на лични данни имат служителите в ПГИИРЕ – 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. 17. Служителите в ПГИИРЕ „Михай Еминеску“, на които е предоставен достъп до лични данни, са длъжни да ги обработват законосъобразно и добросъвестно, съобразно целите, за които са събрани, и да не ги обработват допълнително по начин, несъвместим с тези цели, както и да ги съхраняват за срок, който не надхвърля необходимото за целите, за които се обработват.

ДОСТЪП НА ТРЕТИ ЛИЦА ДО РЕГИСТРИТЕ СЪДЪРЖАЩИ ЛИЧНИ ДАННИ

Чл. 18. (1) Достъп до лични данни, обработвани от администратора, се предоставя на държавни и общински органи, институции, организации и други лица, когато това е предвидено в нормативен акт, когато е необходимо за изпълнение на законово установени правомощия или задължения или при наличие на друго приложимо правно основание за обработване и предоставяне на данните.

(2) Предоставянето на лични данни на органи на съдебната власт, органи на изпълнителната власт, контролни и надзорни органи, както и на други компетентни органи, се извършва само в обхвата на необходимите за конкретното производство или проверка данни и при спазване на приложимите изисквания за защита на личните данни.

(3) При постъпило искане от компетентен държавен или друг оправомощен орган за предоставяне на лични данни, същото се изпълнява след проверка на правното основание, компетентността на органа и обхвата на исканите данни. Когато е необходимо, искането следва да съдържа данни за основанията и целта, за които се изискват личните данни.

(4) Предоставянето на лични данни по ал. 1–3 се извършва от директора на училището или от определено от него лице, в рамките на предоставените му правомощия и при спазване на изискванията за законосъобразност, добросъвестност, прозрачност и минимизиране на данните.

(5) Когато предоставянето на лични данни е извършено въз основа на официално искане от компетентен орган, се съхранява документ или друг доказуем запис за предоставените данни, органа, на който са предоставени, основанието и датата на предоставянето, когато това е приложимо.

ВИДОВЕ ЗАЩИТА НА ЛИЧНИ ДАННИ

ЛИЦЕ ПО ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

Чл. 19 (1) За осигуряване на законосъобразното обработване и подходящото ниво на защита на личните данни администраторът определя със заповед длъжностно лице по защита на данните.

(2) Длъжностното лице по защита на данните изпълнява функциите и задачите, предвидени в Регламент (ЕС) 2016/679 и приложимото национално законодателство, като:

- информира и консултира администратора и служителите, които обработват лични данни, относно задълженията им за защита на личните данни;
- наблюдава спазването на изискванията за защита на личните данни и на настоящите вътрешни правила;
- подпомага администратора при определянето и контрола на организационните и техническите мерки за защита на личните данни;
- подпомага администратора при оценяването и управлението на рисковете, свързани с обработването на лични данни;
- участва при установяване и документиране на нарушения на сигурността на личните данни;
- при установяване или получаване на информация за нарушение на сигурността на личните данни уведомява без ненужно забавяне администратора и го подпомага при преценката относно необходимостта от уведомяване на Комисията за защита на личните данни и, когато е приложимо, на засегнатите лица;
- сътрудничи с Комисията за защита на личните данни и изпълнява функциите на лице за контакт по въпросите, свързани със защитата на личните данни;
- информира и обучава периодично служителите по въпросите на защитата на личните данни;
- извършва или подпомага извършването на проверки за спазване на изискванията за защита на личните данни и предлага мерки за отстраняване на установени несъответствия;
- изпълнява и други задачи, предвидени в приложимото законодателство, при условие че те не водят до конфликт на интереси.

(3) При изпълнение на функциите си длъжностното лице по защита на данните спазва изискванията за поверителност и професионална тайна съгласно приложимото законодателство.

Чл. 20. (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) В училището се прилагат следните основни видове защита:

- Физическа защита – мерки за контрол на достъпа до сградата, помещенията, шкафове, съоръженията и другите места, в които се обработват или съхраняват лични данни;
- Персонална защита – организационни мерки по отношение на служителите и другите лица, на които е предоставен достъп до лични данни във връзка със служебните им задължения;
- Документална защита – мерки за защита на личните данни, съдържащи се в документи на хартиен носител, включително правила за достъп, съхранение, използване и предоставяне;
- Защита на информационните системи и електронните данни – подходящи технически и организационни мерки за защита на личните данни, обработвани чрез компютри, информационни системи, електронни дневници и други електронни средства;

Мерките за защита се определят и прилагат със заповеди на директора, вътрешни правила, процедури и други организационни документи съобразно конкретните дейности и установените рискове.

Чл. 21 (1) Документи, съдържащи лични данни, се приемат и регистрират по установения в училището ред. При необходимост лицето, което приема документа, предоставя на заявителя информация относно обработването на личните му данни и правата му като субект на данни съгласно приложимото законодателство.

(2) Когато за конкретното обработване е необходимо предоставяне на информация, декларация или друг документ от лицето, същите се представят в предвидената от закона или вътрешните правила форма. Не се изисква отделно съгласие, когато обработването се извършва на друго приложимо правно основание.

(3) При необходимост лицето, приемащо документите, може да извърши проверка на самоличността или на представителната власт на лицето, когато това е необходимо за законосъобразното обработване на личните данни.

(4) Внесените документи с лични данни се предоставят на директора или на определено от него лице за разпределяне към служителите, чиито служебни задължения налагат достъп до съответните данни.

(5) Лицата, на които е предоставен достъп до лични данни, обработват същите само в рамките на предоставените им права и служебни задължения и при спазване на изискванията за поверителност и защита на личните данни.

(6) Лични данни се предоставят на трети лица само при наличие на приложимо правно основание и от лица, определени от директора съобразно предоставените им правомощия.

(7) Когато е необходимо, при предоставяне на лични данни на трети лица се документират основанията, целта, обхватът на предоставените данни, получателят и датата на предоставянето.

МЕРКИ ЗА ЗАЩИТА ПРИ ОБРАБОТВАНЕ НА ЛИЧНИТЕ ДАННИ

Чл. 22. (1) При обработването на лични данни в ПГИИРЕ „Михай Еминеску“ се прилагат подходящи технически и организационни мерки за защита на данните от неправомерен достъп, загуба, унищожаване, изменение, неправомерно разкриване или друг вид незаконно обработване.

(2) Мерките за защита се прилагат съобразно вида на обработваните данни, начина на обработване, използваните носители и информационни системи и установените рискове.

(3) При обработване на лични данни на хартиен носител се прилагат мерки за:

- ограничаване на достъпа до документите и помещенията, в които се съхраняват;
- съхраняване на документите по начин, който не допуска достъп от неоторизирани лица;
- предотвратяване на загуба, повреждане или неправомерно унищожаване;
- предоставяне на документите само на лица, за които достъпът е необходим за изпълнение на служебните им задължения.

(4) При електронно обработване на лични данни се прилагат подходящи мерки за:

1. ограничаване на достъпа до информационни системи, електронни файлове и други ресурси, съдържащи лични данни;
2. използване на индивидуални потребителски профили и пароли, когато такива са предвидени от съответната система;
3. предоставяне на достъп само до необходимите за служебните задължения данни;
4. предотвратяване на неправомерно копиране, изменение, изтриване или предоставяне на лични данни;
5. защита на данните при тяхното предаване и обмен чрез електронни средства.

(5) При обработване на лични данни чрез информационни системи, електронен дневник и други електронни средства се спазват и правилата за сигурност и достъп, определени от съответния администратор на системата и приложимите нормативни изисквания.

Чл. 23. (1) Служителите, на които е предоставен достъп до лични данни, са длъжни да спазват определените правила и мерки за защита и да не предоставят достъп до лични данни на неоторизирани лица.

(2) При електронно обработване на лични данни служителите:

- не предоставят своите потребителски имена, пароли и други средства за идентификация на други лица;
- не оставят без надзор отворени информационни системи или документи, съдържащи лични данни, когато това може да доведе до неправомерен достъп;
- не копират, променят, изтриват или предоставят лични данни извън предоставените им права и служебни задължения;
- спазват правилата за сигурност, определени за използваните информационни системи и електронни ресурси.

(3) При установяване на загуба, неправомерен достъп, погрешно предоставяне, неправомерно разкриване или друго съмнение за нарушение на сигурността на личните данни служителят уведомява без ненужно забавяне директора и длъжностното лице по защита на данните.

(4) При обработване на лични данни служителите са длъжни да спазват принципите за законосъобразност, добросъвестност, прозрачност, минимизиране на данните, точност и ограничение на съхранението.

ОЦЕНКА НА ВЪЗДЕЙСТВИЕТО ВЪРХУ ОБРАБОТВАНИТЕ ЛИЧНИ ДАННИ

Чл. 24. (1) Оценката на въздействието върху защитата на личните данни представлява процес за установяване, оценяване и управление на рисковете за правата и свободите на физическите лица, свързани с конкретно обработване на лични данни.

(2) Администраторът извършва оценка на въздействието, когато предвиденото обработване, по-специално при използване на нови технологии, вероятно ще доведе до висок риск за правата и свободите на физическите лица, като се отчитат естеството, обхватът, контекстът и целите на обработването.

(3) Оценката на въздействието се извършва преди започване на съответното обработване, когато това се изисква от приложимото законодателство.

(4) При извършване на оценката на въздействието администраторът се консултира с длъжностното лице по защита на данните, когато такова е определено.

(5) Оценката на въздействието се преразглежда при необходимост, когато настъпи промяна в обработването, използваните технологии, целите, обхвата или рисковете, които могат да повлияят върху правата и свободите на физическите лица.

Чл. 25. (1) При преценката за необходимостта от извършване на оценка на въздействието администраторът отчита по-специално следните обстоятелства:

- систематична и подробна оценка на лични аспекти на физически лица, основана на автоматизирано обработване, включително профилиране, когато въз основа на нея се вземат решения с правни последици или решения, които по подобен начин значително засягат лицата;
- мащабно обработване на специални категории лични данни, включително данни за здравословното състояние, както и на лични данни, свързани с присъди и нарушения;
- систематично наблюдение на публично достъпна зона в голям мащаб;
- използване на нови технологии или въвеждане на нови технологични или организационни решения, когато това може да доведе до висок риск за правата и свободите на физическите лица;
- обработване на лични данни на голям брой лица или обработване на данни на лица, които могат да се намират в уязвимо положение, когато това създава висок риск;
- комбиниране или съпоставяне на различни масиви от лични данни, когато това може да доведе до висок риск;
- други случаи, при които съобразно приложимото законодателство или указанията на Комисията за защита на личните данни се изисква извършване на оценка на въздействието.

(2) При обработването на лични данни чрез видеонаблюдение администраторът извършва преценка дали конкретното обработване е вероятно да доведе до висок риск за правата и свободите на физическите лица и дали са налице условия за извършване на оценка на въздействието съгласно приложимото законодателство.

(3) Когато в резултат на оценката се установи висок риск, който не може да бъде ограничен чрез подходящи технически и организационни мерки, администраторът предприема действия съгласно приложимото законодателство, включително когато е приложимо, извършва предварителна консултация с Комисията за защита на личните данни.

ОЦЕНЯВАНЕ НА РИСКА И ОПРЕДЕЛЯНЕ НА ПОДХОДЯЩИ МЕРКИ ЗА ЗАЩИТА

Чл. 26. (1) Администраторът оценява рисковете за правата и свободите на физическите лица при обработването на лични данни с оглед определяне на подходящи технически и организационни мерки за тяхната защита.

(2) При оценяването на риска се вземат предвид естеството, обхватът, контекстът и целите на обработването, категориите лични данни и субекти на данни, начинът на обработване и съхранение, използваните технологии и възможните последици при нарушение на сигурността.

(3) При оценяването се отчитат рисковете от случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или достъп до лични данни.

Чл. 27. (1) За всеки регистър и дейност по обработване на лични данни се определят подходящи технически и организационни мерки съобразно установените рискове.

(2) При определяне на мерките се отчитат необходимостта от гарантиране на поверителност, цялостност и наличност на личните данни, както и възможността за своевременно възстановяване на достъпа до тях при инцидент.

(3) Оценката на риска и подходящите мерки за защита се преразглеждат при промени в обработването, използваните технологии, категориите или обема на данните, както и при възникване на нови рискове.

Чл. 28. (1) Мерките за защита на личните данни се определят и прилагат съобразно принципа на сигурност на обработването и установените рискове.

(2) При обработване на специални категории лични данни, данни на деца и други данни, при които съществува повишен риск за правата и свободите на физическите лица, се прилагат допълнителни подходящи мерки, когато това е необходимо.

Чл. 29. (1) Ефективността на прилаганите технически и организационни мерки се проверява и оценява периодично, както и при необходимост.

(2) При установяване на недостатъчна защита или повишаване на риска се предприемат действия за подобряване на мерките за защита.

(3) Длъжностното лице по защита на данните подпомага оценяването и преразглеждането на рисковете и мерките за защита в рамките на предоставените му правомощия.

ПРОЦЕДУРИ ЗА ДОКЛАДВАНЕ И УПРАВЛЕНИЕ ПРИ ИНЦИДЕНТИ

Чл. 30. (1) При възникване и установяване на инцидент и/или нерегламентиран достъп, свързан с нарушаване защитата или загубата на лични данни, незабавно се докладва на лицето по защита на личните данни в ПГИИРЕ.

(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 действията по възстановяването се извършват от определени със заповед на директора лица или от лица, на които е предоставен съответният служебен достъп, при спазване на приложимите правила за сигурност и се документират, когато това е необходимо.

(5) В случаите на компрометиране на парола, тя се подменя с нова, като събитието се отразява в регистъра за инциденти.

ОТГОВОРНОСТ

Чл. 31. За неизпълнение на задълженията, вменени на съответните оправомощени лица по тези Правила, по ЗЗЛД и по Регламент (ЕС) 2016/679 на Европейския съюз, се налагат дисциплинарни наказания по КТ, а когато неизпълнението на съответното задължение е констатирано и установено от надлежен орган – предвиденото в ЗЗЛД административно наказание.

Чл. 32. (1) За вреди, причинени в резултат на незаконосъобразно обработване на лични данни от служители в ПГИИРЕ, 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 или Закона за държавния служител.

За всички неуредени случаи се прилагат разпоредбите на Регламент 2016/679 на Европейския парламент, ЗЗЛД и разпоредженията на Директора на образователната институция-администратор на лични данни.

Настоящите правила са утвърдени със заповед №665/14.09.2026 г.

Данни за контакт на длъжностното лице по защита на данните според ЗЗЛД:

Емил Асенов Георгиев, тел. 0878151020