ПРОФЕСИОНАЛНА ГИМНАЗИЯ ПО ИКОНОМИКА “ИВАН ИЛИЕВ” - БЛАГОЕВГРАД
2700 Благоевград, ж.к. “Ален мак”, тел. 885288, 885289, www.pgiblg.com

И Н С Т Р У К Ц И Я

ЗА МЕРКИТЕ И СРЕДСТВАТА ЗА ОБРАБОТВАНЕ И ЗАЩИТА НА ЛИЧНИ ДАННИ

В ПГИ „ИВАН ИЛИЕВ“

ГРАД БЛАГОЕВГРАД

Глава първа
ОБЩИ ПОЛОЖЕНИЯ

Чл. 1. **(1)** С тази инструкция 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) Настоящата инструкция се издава на основание Регламент (ЕС) 2016/679 и Закона за защита на личните данни (ЗЗЛД).

(3) Инструкцията се утвърждава, допълва, изменя и отменя от Директора на ПГИ „Иван Илиев“ – администратор на лични данни.

(4) Администраторът предоставя достъп до обработваните от него лични данни на физическите лица и на трети лица съобразно Регламент (ЕС) 2016/679 на ЕС и ЗЗЛД.

Глава втора
ЦЕЛИ И ОБХВАТ НА ИНСТРУКЦИЯТА

Чл. 2. Настоящата инструкция има за цел да регламентира:

(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. Инструкцията е задължителна за всички лица имащи достъп до личните данни, обработвани за нуждите на администратора.

Глава трета
СУБЕКТИ НА ЛИЧНИ ДАННИ.
ПРАВА НА СУБЕКТИТЕ НА ЛИЧНИТЕ ДАННИ.

Чл. 4. (1) Субект на лични данни е физическото лице, за което тези лични данни се отнасят.

(2) Субекти на лични данни в Училището са:

1. работниците и служителите, работещи по трудови правоотношения с Училището;

2. учениците, записани в различните форми на обучение в Училището;

3. родителите на учениците, записани в училището, чиито лични данни се обработват от Училището;

4. физически лица, с които Училището има сключени граждански договори или са представители на юридически лица, с които училището е в договорни отношения;

5. други физически лица, чиито данни се обработват от Училището във връзка с осъществяване на цялостната дейност на Училището.

Право на достъп

Чл. 5. (1) Субект на лични данни има право да получи потвърждение от Училището дали се обработват негови лични данни.

(2) Когато Училището обработва лични данни на субекта, той - субектът на лични данни има право до получи достъп до личните си данни.

(3) В случаите по ал. 2 субектът на лични данни има право да получи и информация относно:

1. целите на обработването;

2. съответните категории лични данни;

3. получателите или категориите получатели, пред които са или ще бъдат разкрити личните данни;

4. предвидения срок, за който ще се съхраняват личните данни, а ако това е невъзможно, критериите, използвани за определянето на този срок;

5. съществуването на право да се изиска от Училището коригиране или изтриване на личните данни на субекта или ограничаване на обработването на личните данни на субекта или да се направи възражение срещу такова обработване;

6. когато личните данни не се събират от субекта на данните, всякаква налична информация за техния източник;

7. съществуването на автоматизирано вземане на решения, включително профилирането и съществена информация относно използваната логика, както и значението и предвидените последствия от това обработване за субекта на личните данни.

Право на коригиране

Чл. 6. (1) Субектът на лични данни има право да поиска от Училището да коригира без ненужно забавяне неточните лични данни, свързани с него.

(2) Субектът на лични данни има право предвид целите на обработването да поиска от Училището да попълни личните му данни, когато те са непълни.

(3) Искането по ал. 2 може да се направи чрез внасяне на декларация.

Право на изтриване (право „да бъдеш забравен")

Чл. 7. (1) Субектът на лични данни има право да поиска от Училището без ненужно забавяне да изтрие (да заличи) свързаните с него лични данни

(2) В случаите по ал. 1 Училището е длъжно да изтрие (да заличи) личните данни на субекта когато е приложимо някое от основанията както следва:

1. личните данни повече не са необходими за целите, за които са били събрани или обработвани

2. субектът на лични данни оттегля своето съгласие, върху което се основава обработването на личните ми данни;

3. субектът на лични данни възразява срещу обработването им и няма законни основания за обработването им, които да имат преимущество пред възражението на субекта;

4. личните данни са били обработвани незаконосъобразно;

5. личните данни трябва да бъдат изтрити с цел спазването на правно задължение, произтичащо от Регламента, ЗЗДЛ и подзаконовите нормативни актове по прилагането му.

(3) Когато Училището е направило личните данни на субекта обществено достояние и е длъжно в условията на ал. 1 и ал. 2 да ги изтрие (да ги заличи), Училището като отчита наличната технология и разходите по изпълнението, предприема разумни стъпки, включително технически мерки, за да уведоми администраторите, обработващи личните данни, че субектът на данните е поискал изтриване от тези администратори на всички връзки, копия или реплики на тези лични данни.

Право на ограничаване на обработването

Чл. 8. (1) Субектът на лични данни има право да поиска от Училището да ограничи обработването на личните му данни, при наличие на едно от следните основания:

1. точността на личните данни се оспорва от субекта на лични данни, за срок, който позволява на Училището да провери точността на личните данни;

2. обработването е неправомерно, но субектът на лични данни не желае личните му данни да бъдат изтрити, а изисква вместо това ограничаване на използването им;

3. Училището не се нуждае повече от личните данни за целите на обработването, но субектът на лични данни ги изисква за установяването, упражняването или защитата на негови правни претенции;

4. субектът на лични данни е възразил срещу обработването на личните му данни в очакване на проверка дали законните основания на Училището имат преимущество пред интересите на субекта на данните.

(2) В случаите по ал. 1. Училището обработва личните данни само със съгласието на субекта на лични данни или в случай на необходимост за установяването, упражняването или защитата на правни претенции или за защита на правата на друго физическо лице или поради важни основания от обществен интерес.

(3) В случаите по ал. 1 Училището информира субекта преди отмяната на ограничаването на обработването.

Чл. 9. (1) Училището е длъжно да информира всеки получател, на когото личните данни на един субект или субекти са били разкрити за всяко извършено в съответствие с чл. 7, чл. 8 и чл. 9 от Инструкцията коригиране, изтриване или ограничаване на обработването на личните данни на този дин субект или субекти, освен ако това е невъзможно или изисква несъразмерно големи усилия.

(2) Училището е длъжно да информира субекта на лични данни за получателите на личните му данни по ал. 1 само, ако субектът на лични данни е поиска това.

Право на преносимост на данните

Чл. 10. (1) Субектът на лични данни има право да получи личните данни, които го засягат и които той е предоставил на Училището, в структуриран, широко използван и пригоден за машинно четене формат и има правото да прехвърли тези данни на друг администратор на лични данни без възпрепятстване от Училището когато:

1. обработването е основано на съгласие на субекта на лични данни или на договорно задължение;

2. обработването се извършва по автоматизиран начин.

(2) В случаите по ал. 1 субектът на лични данни има право да получи пряко прехвърляне на личните му данни от Училището към друг администратор на лични данни, когато това е технически осъществимо.

(3) правото по ал. 1. не се отнася до обработването, необходимо за изпълнението на задачи от обществен интерес или при упражняването на официални правомощия, които са предоставени на администратора.

Право на възражение

Чл. 11. (1) Субектът на лични данни има право, по всяко време и на основания, свързани с неговата конкретна ситуация, на възражение срещу обработването на личните му данни, включително профилиране.

(2) В случаите по ал. 1. Училището прекратява обработването на личните данни, освен ако не докаже, че съществуват убедителни законови основания за обработването им, които основания имат предимство пред интересите, правата и свободите на субекта на лични данни, или за установяването, упражняването или защитата на правни претенции.

(3) Субектът на лични данни трябва а бъде уведомен най-късно в момента на първото осъществяване на контакт с него, за правата му по ал. 1 и ал. 2. Уведомяването трябва да с представи по ясен начин отделно от всяка друга информация.

(4) Субектът на лични данните може да упражнява правото си на възражение чрез автоматизирани средства, като се използват технически спецификации.

(5) Когато лични данни се обработват за целите на научни или исторически изследвания или за статистически цели субектът на личните данни има право, въз основа на конкретното си положение, да възрази срещу обработването на лични данни, отнасящи се до него, освен ако обработването е необходимо за изпълнението на задача, осъществявана по причини от публичен интерес.

Автоматизирано вземане на решения, включително профилиране

Чл. 12. (1) Субектът на лични данни има право да не бъде обект на решение, основаващ се единствено на автоматизирано обработване, включително профилиране, което поражда правни последствия за субекта на личните данни или по подобен начин го засяга в значителна степен.

(2) Правото по ал. 1. не се прилага когато е налице едно от следните условия:

1. решението се основава на изричното съгласие на субекта на лични данни;

2. решението е необходимо за сключването или изпълнението на договор между субект на данни и администратор на лични данни;
3. решението е разрешено от Регламента, ЗЗЛЗ и подзаконовите нормативни актове по неговото прилагане.
(3) В случаите по ал. 2 в Училището се предвиждат подходящи мерки за защита на правата и свободите, и легитимните интереси на субекта на данните.

Глава четвърта
АДМИНИСТРАТОР НА ЛИЧНИ ДАННИ. ОБРАБОТВАЩ ЛИЧНИ ДАННИ. ЗАДЪЛЖЕНИЯ НА АДМИНИСТРАТОРА И НА ОБРАБОТВАЩИЯ ЛИЧНИТЕ ДАННИ.

Чл. 13. (1) Като администратор на лични данни Училището само определя целите и средствата за обработването на лични данни в съответствие с Регламента, ЗЗДЛ и подзаконовите нормативни актове по прилагането му.
(2) Като взема предвид естеството, обхвата, контекста и целите на обработването, както и рисковете с различна вероятност и тежест за правата и свободите на физическите лица, Училището като администратор на лични данни въвежда и при необходимост актуализира подходящи технически и организационни мерки, за да гарантира и да е в състояние да докаже, че обработването на лични данни се извършва в съответствие с Регламента, ЗЗЛД и подзаконовите нормативни актове по неговото прилагане.
(3) Когато това е пропорционално на дейностите по обработване на личните данни, мерките по ал. 2 включват прилагане от страна на Училището като администратор на лични данни на подходящи политики за защита на личните данни, които обработва.

Чл. 14. (1) Обработващ лични данни е физическо лице, което обработва лични данни от името на администратора.
(2) Обработващите лични данни в Училището се определят със заповед на директора на училището.

Чл. 15. (1) Обработващите лични данни в Училището предоставят достатъчни гаранции за прилагането на подходящи технически и организационни мерки по такъв начин, че обработването да протича в съответствие с изискванията на Регламента, ЗЗЛД и подзаконовите нормативни актове по неговото прилагане.
(2) Обработващите лични данни в Училището осигуряват защита на правата на субектите на лични данни.

Чл. 16. (1) Обработващите лични данни в Училището:
1. обработва личните данни само по документирано нареждане на администратора;
2. поемат ангажимент за поверителност, за което подписват изрична декларация;

3. като взема предвид естеството на обработването, подпомага Училището, чрез подходящи технически и организационни мерки при изпълнението на задължението на Училището да гарантира правата на субектите на лични данни, установени в глава втора от настоящата Инструкция;

4. подпомага Училището да гарантира изпълнението на задълженията за:

4.1. сигурност на обработването;

4.2. уведомяване на надзорния орган за нарушения в сигурността на личните данни;

4.3. съобщаване на субектите на лични данни за нарушения в сигурността на личните им данни;

4.4. оценката на въздействието върху защитата на личните данни;

4.5. предварителни консултации с надзорния орган, като отчита естеството на обработване и информацията, до която е осигурен достъп на обработващия лични данни;

5. по решение на Училището в случай на прекратяване на трудовото му правоотношение с Училището заличава или връща всички лични данни и заличава съществуващите копия, освен ако Регламента или действащото законодателство в България , не изискват тяхното съхранение;

6. осигурява достъп на Училището до цялата информация, необходима за доказване на изпълнението на задълженията, определени в настоящия член, и позволява и допринася за извършването на одити.

(2) Обработващите лични данни носят отговорност за виновно неизпълнение на изброените в ал. 1 задължения.

Чл. 17. Обработващият лични данни и всяко лице, действащо под ръководството на Училището като администратор на лични данни или на обработващия лични данни, което има достъп до личните данни, обработва тези данни само по указание на Училището и при стриктното спазване на Регламента, ЗЗЛД и подзаконовите нормативни актове по неговото прилагане.

Глава пета

ОБРАБОТВАНЕ ЛИЧНИ ДАННИ В ПГИ „ИВАН ИЛИЕВ“

Раздел I

РЕГИСТРИ

Предназначение и видове регистри

Чл. 18. (1) Училището като администратор на лични данни поддържа регистри на дейностите по обработване на личните данни, които съдържат:

1. наименованието на Училището и координати за връзка;

2. имената на длъжностното лице по защита на данните и координати за връзка;

3. целите на обработване на личните данни;

4. описание на категориите субекти на лични данни;

5. категориите лични данни, които се обработват;

6. категориите получатели на лични данни, пред които се разкриват лични данни: РУО - Благоевград, ДАЗД, КЗЛД, Общинска администрация и други контролни органи при извършване на проверки в Училището във връзка с техните правомощия;

7. когато е възможно, предвидените срокове за изтриване на различни категории данни;

8. когато е възможно, общо описание на техническите и организационни мерки за сигурност при обработване на личните данни.

(2) Подробно описание на регистрите включително категории физически лица, за които се обработват лични данни, групи обработвани данни, източници и средства за събирането им, форма за водене на регистъра, ред за съхраняване и унищожаване на информационни носители, служители, обработващи лични данни, техническите ресурси, прилагани за обработване на данните в електронните регистри и други се съдържа в Приложенията, неразделна част от настоящата Инструкция.

(3) Създаването на нови регистри и извършването на промени се извършва със заповед на Директора на Администратора.

Чл. 19. Обработващият лични данни поддържа регистър на всички категории дейности по обработването на личните данни, обработвани от името на Училището, който съдържа:

1. имената на обработващия личните данни и координати за връзка;

2. имената на длъжностното лице по защита на данните и координати за връзка;

3. категориите на обработване на личните данни;

4. когато е възможно, общо описание на техническите и организационни мерки за сигурност при обработване на личните данни.

Чл. 20. Регистрите по чл. 19 и чл. 20 се поддържат в писмена форма и в електронен формат.

Форми на водене на регистрите

Чл. 21. (1) Формите на водене на регистрите биват 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 картотечния шкаф – учителска стая, дирекция, канцелария заместник-директори, канцелария ЗАС, счетоводство.

(2) Носител (форма) за предоставяне на данните от физическите лица – хартиен. Личните данни от лицата се подават на администратора на лични данни и оправомощеното лице, назначено за обработването им – обработващ лични данни, на основание нормативно задължение във всички случаи, когато е необходимо.

1. Достъп до личните данни – такъв има само обработващият лични данни.

(3) Водене на регистър на технически носител:

1. Форма на организация и съхраняване на личните данни – личните данни се съхраняват на твърд диск, на изолиран компютър;

2. Местонахождение на компютъра – канцелария на заместник-директорите, счетоводство, канцелария на ЗАС;

3. Достъп до личните данни и защита - достъп до операционната система, съдържаща файлове за обработка на лични данни, има само обработващият лични

данни чрез парола за отваряне на тези файлове, както и длъжностното лице по защита на личните данни посредством делегирани му права и задължения от администратора на лични данни.

Групи данни в регистрите

Чл. 22. **(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 – здравен 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.

Задължения на лицето, отговарящо за водене и съхраняване на данните в регистрите

Чл. 23. Задълженията на лицето, отговарящо за водене и съхраняване на данните в регистъра (оправомощеното лице) включват набиране, обработване, актуализация и съхраняване на лични данни.

Периодично архивиране

Чл. 24. Архивиране на личните данни на технически носител се извършва периодично на всеки 5 (пет) години от обработващия лични данни с оглед запазване на информацията за съответните лица в актуален вид.

Контрол при обработване на личните данни

Чл. 25. Контролът върху дейностите по обработка на лични данни се осъществява от длъжностно лице по защита на личните данни.

Актуализация на лични данни

Чл. 26. (1) Актуализация на лични данни представлява допълнение или изменение на съществуваща информация в дружеството. Актуализация на лични данни се извършва:

1. по искане на лицето, за което се отнасят личните данни, когато то е установило, че е налице грешка или непълнота в тях, и удостовери това с документ;

2. по инициатива на обработващия лични данни – при наличие на документ, даващ основание за актуализация;

3. при установена грешка при обработката на личните данни от страна на ПГИ „Иван Илиев";

(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.

Раздел II
СИГУРНОСТ ПРИ ОБРАБОТВАНЕТО НА ЛИЧНИТЕ ДАННИ

Чл. 27. (1) Като се имат предвид достиженията на техническия прогрес, разходите за прилагане и естеството, обхватът, контекстът и целите на обработването на личните данни, както и рисковете с различна вероятност и тежест за правата и свободите на субектите на лични данни, Училището и определеният със заповед на директора на училището обработващ лични данни, прилагат подходящи технически и организационни мерки за осигуряване на съобразено с този риск ниво на сигурност.

(2) Технически и организационни мерки за осигуряване на сигурност в обработването на личните данни, които Училището предприема, имат за цел:

1. гарантиране на постоянна поверителност, цялостност, наличност и устойчивост на системите и услугите за обработване;

2. своевременно възстановяване на наличността и достъпа до личните данни в случай на физически или технически инцидент;

3. редовно изпитване, преценяване и оценка на ефективността на предприетите техническите и организационните мерки

Чл. 28. (1) Технически и организационни мерки за осигуряване на сигурност в обработването на личните данни в Училището са:

1. Псевдонимизация - обработването на лични данни се извършва по такъв начин, че личните данни не могат повече да бъдат свързвани с конкретен субект на данни, без да се използва допълнителна информация, при условие че тази допълнителна информация се съхранява отделно;

2. Криптиране – обработването на лични данни се извършва по начин, при който личните данни се шифрират и не могат повече да бъдат разкрити без наличието на използвания за шифрирането код (шифър), който се съхранява отделно.

(2) Конкретните технически и организационни мерки за осигуряване на сигурност се определят в зависимост от категорията лични данни, които се обработват.

(3) При определяне на технически и организационни мерки за осигуряване на сигурност се взима предвид рисковете от случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или достъп до прехвърлени, съхранявани или обработени по друг начин лични данни.

Глава шеста

ДОСТЪП ДО ЛИЧНИ ДАННИ

Раздел I

Осигуряване на достъп на лицата до личните им данни

Чл. 29. **(1)** Всяко физическо лице, както и служителите в ПГИ „Иван Илиев“, 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. 30. (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. 31. (1) Молбата 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 молба от упълномощено лице към същото се прилага и нотариално заверено пълномощно.

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

Чл. 32. (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. 33. (1) Администраторът на лични данни или изрично оправомощено от него лице разглежда молбата по чл. 11 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 й.

Чл. 34. Право на достъп до данните в поддържаните от администратора регистри на лични данни имат служителите в ПГИ „Иван Илиев" – 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. 35. Служителите в ПГИ „Иван Илиев" 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.

Раздел II

Достъп на трети лица до регистрите, съдържащи лични данни

Чл. 36. (1) Достъп до обработваните от администратора лични данни имат лицата, за които същия произтича от законово или договорно основание, както и органи 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 непозволени увреждания. На такива лица се осигурява достъп до личните данни, като при необходимост им се осигуряват съответни условия за работа в помещение на детската градина/ училището.

(3) Правомерен е и достъпът на ревизиращите държавни органи, надлежно легитимирали 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 седма

ВИДОВЕ ЗАЩИТА НА ЛИЧНИ ДАННИ

Лицата по защита на личните данни

Чл. 37. (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 ПГИ „Иван Илиев;

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. 38. (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.

6. Мерките на различните видове защита се определят съгласно приложение № 6 от настоящите Правила.

Чл. 39 (1) Всяко лице желаещо да внесе документ съдържащ лични данни предоставя същия в деловодството на ПГИ „Иван Илиев“. Лицето приемащо документа е задължено да запознае вносителят на документите с правата му на субект на лични данни, както и с Инструкцията 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.

Мерки за защита при обработване на личните данни

Чл. 40. (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. 41. (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 осма
ОЦЕНКА НА ВЪЗДЕЙСТВИЕТО ВЪРХУ ОБРАБОТВАНИТЕ ЛИЧНИ ДАННИ

Чл. 42. (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. 43. 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. 44. 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. 45. (1) Администраторът извършва оценка на въздействие за всички поддържани регистри .

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

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

Чл. 46. В зависимост от нивото на въздействие се определя и съответно ниво на защита.

Чл. 47. (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 девета
ПРОЦЕДУРИ ЗА ДОКЛАДВАНЕ И УПРАВЛЕНИЕ ПРИ ИНЦИДЕНТИ

Чл. 48. (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 ПГИ „Иван Илиев".

(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.

Чл. 49. Обработващият лични данни уведомява Училището като администратор на лични данни без ненужно забавяне, след като узнае за нарушаване на сигурността на лични данни.

Чл. 50. (1) В случай на нарушение на сигурността на личните данни Училището, без ненужно забавяне и когато това е осъществимо — не по-късно от 72 часа след като е разбрал за него, уведомява за нарушението на сигурността на личните данни съответния надзорния орган.

(2) Уведомлението по ал. 1 съдържа най-малко:

1. описание на естеството на нарушението на сигурността на личните данни, включително, ако е възможно, категориите и приблизителният брой на засегнатите субекти на лични данни и категориите и приблизителното количество на засегнатите записи на лични данни;

2. посочване на името и координатите за връзка на длъжностното лице по защита на данните или на друга точка за контакт, от която може да се получи повече информация;

3. описание на евентуалните последици от нарушението на сигурността на личните данни;

4. описание на предприетите или предложените от Училището мерки за справяне с нарушението на сигурността на личните данни, включително по целесъобразност мерки за намаляване на евентуалните неблагоприятни последици.

Чл. 51. (1) Когато има вероятност нарушението на сигурността на личните данни да породи висок риск за правата и свободите на субектите на лични данни, Училището, без ненужно забавяне, съобщава на субекта на личните данните за нарушението на сигурността на личните данни.

(2) Съобщение по ал. 1 не се изисква когато е налице едно от следните условия:

1. Училището е предприело подходящи технически и организационни мерки за защита и тези мерки са били приложени по отношение на личните данни, засегнати от нарушението на сигурността на личните данни, по- специално мерките, които правят личните данни неразбираеми за всяко лице, което няма разрешение за достъп до тях, като например криптиране;

2. Училището е взело впоследствие мерки, които гарантират, че повече няма вероятност да се материализира високият риск за правата и свободите на субектите на лични данни;

3. изпращането на съобщението би довело до непропорционални усилия като в този случай се прави публично съобщение или се взема друга подобна мярка, така че субектите на данни да бъдат в еднаква степен ефективно информирани.

(3) В случаите когато Училището все още не е съобщило на субекта на данните за нарушението на сигурността на личните данни, надзорният орган може, след като отчете каква е вероятността нарушението на сигурността на личните данни да породи висок риск, да изиска от администратора да съобщи за нарушението или да реши, че е изпълнено някое от условията по ал. 2.

Глава
ОТГОВОРНОСТ

Чл. 52. 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. 53. (1). За вреди, причинени в резултат на незаконосъобразно обработване на лични данни от служители в ПГИ „Иван Илиев", 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.

Глава единадесета

ПРЕХОДНИ И ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§ 1. За всички неуредени с настоящата Инструкция въпроси се прилага Регламента, ЗЗЛД, подзаконовите нормативни актове по неговото прилагане и разпорежданията на Директора на образователната институция- администратор на лични данни.

.

§ 2. Настоящите изменения и допълнения на Инструкция са утвърдени със Заповед № РД08-1114/25.05.2018 год. на директора на ПГИ "Иван Илиев"- Благоевград.

§ 3. Изменения и допълнения в настоящата Инструкция се извършват по реда на неговото утвърждаване.

УТВЪРЖДАВАМ:
ДИРЕКТОР:
/Ася Бояджиева – Пенкова/