ИНСТРУКЦИЯ ВЪВ ВРЪЗКА С ОБРАБОТВАНЕТО И ОПАЗВАНЕТО НА ЛИЧНИТЕ ДАННИ В СУ „СВЕТИ ПАТРИАРХ ЕВТИМИЙ“ ГР. ПЛОВДИВ

Глава първа
ОБЩИ ПОЛОЖЕНИЯ

Чл. 1. (1) Инструкцията във връзка с обработването и опазването на личните данни в СУ „Свети Патриарх Евтимий“ – гр. Пловдив (Инструкцията) има за цел да допринесе за правилното прилагане на Регламент (ЕС) 2016/679 на Европейския парламент и на съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Регламента).

(2) Инструкцията има за цел и правилното прилагане на националното законодателство в областта на опазването на личните данни.

(3) Инструкцията отчита специфичните характеристики на сектор „Образование“ и конкретните нужди на СУ „Свети Патриарх Евтимий“ – гр. Пловдив (Училището).

Чл. 2. (1) Инструкцията е съобразена с Регламента и действащите нормите на Закона за защита на личните данни (ЗЗДЛ) и подзаконовите нормативни актове по прилагането му

(2) Инструкцията не може да противоречи на Регламента и на действащите нормите на Закона за защита на личните данни и подзаконовите нормативни актове по прилагането му. При наличие на противоречие се прилагат нормите на Регламента, ЗЗДЛ и подзаконовите нормативни актове по прилагането му.

(3) Инструкцията се актуализира при изменения и допълнения на ЗЗЛД и подзаконовите нормативни актове по прилагането му, които изменения и допълнения се отразяват на съдържанието му.

Чл. 3. (1) Лични данни са всяка информация, свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано пряко или непряко, по-специално чрез идентификатор като име, идентификационен номер, данни за местонахождение, онлайн идентификатор или по един или повече признаци, специфични за физическата, физиологичната, генетичната, психическата, умствената, икономическата, културната или социална идентичност на това физическо лице.

(2) Личните данни на физическите лица са:

1. имената (собствено, бащино и фамилно) на лицето и/или прякор

2. Единен граждански номер (ЕГН)

3. адрес (постоянен или настоящ)

4. паспортни данни / данни за личната карта на лицето (физическа идентичност)

5. семейно положение и/или родствени връзки (семейна идентичност)

6. професионална биография (трудова идентичност)

7. здравен статус, психологическо и/или умствено състояние (медицински данни)

8. етнически произход и/или расов произход

9. политически, религиозни и/или философски убеждения (обществена идентичност)

10. имотно и/или финансово състояние (икономическа идентичност)

11. сексуална ориентация

12. други данни, които позволяват идентификацията на физическото лице.

Чл. 4. (1) Училището, като самостоятелно юридическо лице, е администратор на лични данни.

(2) 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.

(3) По-долу в Инструкцията правата и задължението на Училището се разглеждат в качеството му на администратор на лични данни.

Глава втора

СУБЕКТИ НА ЛИЧНИ ДАННИ.

ПРАВА НА СУБЕКТИТЕ НА ЛИЧНИТЕ ДАННИ.

Чл. 5. (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. 6. (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. 7. (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. 8. (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 му 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. 9. (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. 10. (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. 11. (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 аддминистратор 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. 12. (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. 13. (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 трета

АДМИНИСТРАТОР НА ЛИЧНИ ДАННИ, ОБРАБОТВАЩ ЛИЧНИ ДАННИ. ЗАДЪЛЖЕНИЯ НА АДМИНИСТРАТОРА И НА ОБРАБОТВАЩИЯ ЛИЧНИТЕ ДАННИ.

Чл. 14. (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. 15. (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. 16. (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. 17. (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. 18. 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 четвърта
ОБРАБОТВАНЕ ЛИЧНИ ДАННИ В СУ „СВЕТИ ПАТРИАРХ ЕВТИМИЙ“.

Раздел I
РЕГИСТРИ

Чл. 19. (1) Училището като администратор на лични данни поддържа регистър на личните данни, които обработва.

(2) Училището като администратор на лични данни поддържа и регистър на дейностите по обработване на личните данни, който съдържа:

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 – Пловдив, 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;

Чл. 20. 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. 21. Регистрите по чл. 19 и чл. 20 се поддържат в писмена форма и в електронен формат.

Раздел II
СИГУРНОСТ ПРИ ОБРАБОТВАНЕТО НА ЛИЧНИТЕ ДАННИ

Чл. 22. (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. 23. (1) Технически и организационни мерки за осигуряване на сигурност в обработването на личните данни в Училището са:

т. 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;

т. 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.

Чл. 24. (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. 25. Обработващият лични данни уведомява Училището като администратор на лични данни без ненужно забавяне, след като узнае за нарушаване на сигурността на лични данни.

Чл. 26. (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.

ПРЕХОДНИ И ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§ 1. За всички неуредени с настоящата Инструкция въпроси се прилага Регламента, ЗЗЛД и подзаконовите нормативни актове по неговото прилагане.

§ 2. Настоящата Инструкция е утвърдена със заповед №РД-10-1799-1/ 18.05.2018год. на директора на СУ „Свети Патриарх Евтимий“ – гр.Пловдив

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