12. Средно училище „Цар Иван Асен II“
град София, Столична община, район Средец
ул. „Цар Иван Асен II” №72, u_12sou@abv.bg.,тел.02/9437952

ВЪТРЕШНИ ПРАВИЛА

ЗА МЕРКИТЕ И СРЕДСТВАТА ЗА ОБРАБОТВАНЕ И ЗАЩИТА НА ЛИЧНИ ДАННИ НА 12. Средно училище „Цар Иван Асен II“

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 и Закона за защита на личните данни (ЗЗЛД).

(3) Правилата се утвърждават, допълват, изменят и отменят от Директора на 12. Средно училище „Цар Иван Асен II“ – 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

II. 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.

Глава трета

III. Предназначение и видове регистри

Чл. 4. (1) В изпълнение на дейностите си 12 Средно училище „Цар Иван Асен II“ се поддържат следните видове регистри с 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 правоотношения в 12 СУ, определяне на възнагражденията на служителите, здравословни и безопасни условия на труд.

4.1.1.2. Нормативно основание: Кодекс на труда, Кодекс за социално осигуряване, Наредба за трудовата книжка и трудовия стаж, Наредба за пенсиите и осигурителния стаж, Закон за данъците върху доходите на физическите лица, Закон за здравословни и безопасни условия на труд и др.

4.1.1.3. Категории физически лица, за които се обработват данните: персонал (лица по трудово правоотношение или лица по граждански договори), кандидати – участници за назначаване на работа в 12 СУ.

4.1.1.4. Категории лични данни:

- **физическа идентичност –** име, ЕГН, адрес, паспортни данни, месторождение, телефон;
- **физиологична идентичност** – здравен статус (медицинска документация от ЛЛ, ЛКК, ТЕЛК, НЕЛК и други);
- **социална идентичност** – произход, образование, допълнителна квалификация, степени, звания (място, номер и дата на издаване на документите), трудова дейност, професионална автобиография;
- семейна идентичност – семейно положение;
- банкови сметки, свидетелсва за съдимост

4.1.1.5. Източници, от които се събират данните:

- от физическите лица, за които се отнасят данните, с тяхното изрично съгласие (Приложение № 1 към настоящата инструкция);
- от публични регистри (Търговски регистър, Централен регистър на юридическите лица с нестопанска цел за обществено полезна дейност, специални регистри за професионални разрешения, лицензии).

4.1.2. Технологично описание на регистъра

4.1.2.1. Носители на данни

Данните в регистър „Служители“ в 12 СУ се събират и обработват на хартиен носител и в специализиран софтуер на МОН съгласно Наредба № 8 от 11.08.2016г. за информацията и документите за системата на предучилищното и училищното образование.

Хартиените носители на лични данни се съхраняват в кадрови досиета в картотечни шкафове с ключалка. Автоматизираното водене на регистъра се осъществява на компютри със защитен достъп чрез потребителско име и парола. Компютрите са свързани в локална мрежа или са извън нея.

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 на договори, допълнителни споразумения, ведомости за заплати, документи, удостоверяващи трудов стаж, служебни бележки, справки, удостоверения и др.

Обработката на данните се осъществява както на хартиен носител, така и в електронен вид. Личните данни на работещите в 12 СОУ „Цар Иван Асен II” се съхраняват в кабинета на ЗАС.

4.1.2.3. Срок на съхранение

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

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

4.1.2.4. Предоставени услуги

12 СУ не обработва личните данни от регистър „Служители“ за други цели, извън посочените в т. 4.1.1.1.

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 12 СУ, както следва:

- ЗАС;
- счетоводител;
- директор на 12 СУ.

4.2. РЕГИСТЪР „ДОСТАВЧИЦИ“

4.2.1. Общо описание на регистъра

4.2.1.1. Цели на обработване на лични данни: сключване на договори с доставчици с цел обезпечаване материално и технически дейността на 12 СУ, изплащане на възнаграждения за предоставените услуги.

4.2.1.2. Нормативно основание: Закон за обществените поръчки, Правилник за прилагане на закона за обществените поръчки, Закон за задълженията и договорите и др.

4.2.1.3. Категории физически лица, за които се обработват данните: кандидати и участници в обществени поръчки и конкурси, изпълнители по договори.

4.2.1.4. Категории лични данни:

- **физическа идентичност –** име, ЕГН, адрес, телефон;
- **социална идентичност** – образование, допълнителна квалификация, степени, звания (място, номер и дата на издаване на документите), професионална автобиография;
- свидетелсва за съдимост

4.2.1.5. Източници, от които се събират данните:

- от физическите лица, за които се отнасят данните

- от публични регистри (Търговски регистър, Централен регистър на юридическите лица с нестопанска цел за обществено полезна дейност, специални регистри за професионални разрешения, лицензии и други.).

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 компютър с ограничен достъп. Хартиените носители на лични данни се съхраняват в кабинета на директора на 12 СУ. 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 на протоколи за избор на изпълнител за доставки и услуги, граждански договори и други договори за обезпечаване дейността на 12 СУ.

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

4.2.2.3. Срок на съхранение

Данните в регистър „Доставчици“ се съхраняват 5 (пет) години след изпълнението на договорите или до финансова ревизия, освен ако специален закон не изисква съхраняването на отделни документи от тях за по-дълъг срок.

4.2.2.4. Предоставени услуги

12 СУ не обработва личните данни от регистър „Доставчици “ за други цели, извън посочените в т. 4.2.1.1.

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 12 СУ:

- ЗАС;
- домакин;
- счетоводител;
- директор на 12 СУ;

При провеждане на обществени поръчки в обработването на личните данни участват лица – служители, определени със заповед на директора на 12 СУ, в която се посочват задълженията им.

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

4.3. РЕГИСТЪР „УЧАЩИ“

4.3.1. Общо описание на регистъра

4.3.1.1. Цели на обработване на лични данни: За изпълнение на нормативно възложени задължения във връзка с образованието на учениците.

4.3.1.2. Нормативно основание: Закон за предучилищното и училищното образование и произтичащите от него подзаконови актове, Правилник за дейността на 12 СУ „Цар Иван Асен II“.

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

- ученици в 12 СУ;
- кандидати за прием учащи се.

4.3.1.4. Категории лични данни:

- физическа идентичност – име, ЕГН, адрес, месторождение, телефон;

- физиологична идентичност – здравен статус;

- социална идентичност – произход, образование;

- семейна идентичност - семейно положение.

4.3.1.5. Източници, от които се събират данните:

- от физическите лица, за които се отнасят данните;

- от родителите или настойниците.

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 специализиран софтуер на МОН съгласно Наредба № 8 от 11.08.2016 г. за информацията и документите за системата на предучилищното и училищното образование.

4.3.2.2. Технология на обработване

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

Личните данни на учениците се съхраняват в кабинета на секретаря, помощник-директорите, като част от информацията се предоставя на учителите / и чрез дневниците на паралелките/ за изпълнение на служебните им задължения и за евентуална реакция при нужда. Данните на учащите се вписват и на компютри в база данни, съгласно Наредба № 8 от 11.08.2016 г. за информацията и документите за системата на предучилищното и училищното образование, като същите периодично се изпращат в Управленската информационна система на образованието. Компютрите са свързани в локална мрежа или са извън нея.

Помещенията, в които се обработва и съхранява регистърът са с ограничен достъп, оборудвани са със заключващи се шкафове, а достъпът до компютрите се осъществява чрез потребителско име и парола.

4.3.2.3. Срок на съхранение

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

4.3.2.4. Предоставени услуги

12 СУ не обработва личните данни от регистър „Ученици“ за други цели, извън посочените в т. 4.3.1.1.

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 12 СУ:

- ЗАС;

- секретар;

- заместник-директори;

- учители;

- директора на 12 СУ.

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

4.4. РЕГИСТЪР „РОДИТЕЛИ и НАСТОЙНИЦИ“

4.4.1. Общо описание на регистъра

4.4.1.1. Цели на обработване на лични данни: За изпълнение на нормативно възложени задължения във връзка с обучението на учащите и за реализиране на техните права и правата на родителите им.

4.4.1.2. Нормативно основание: Закон за предучилищното и училищното образование и произтичащите от него подзаконови актове, Правилник за прилагане на Закона за семейните помощи за деца

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

- родители;
- настойници.

4.4.1.4. Категории лични данни:

- **физическа идентичност –** име, ЕГН, адрес, телефон.
- **социална идентичност** – произход, образование, месторабота, финансово състояние;
- **семейна идентичност** – семейно положение;
- банкови сметки

4.4.1.5. Източници, от които се събират данните:

-- от физическите лица, за които се отнасят данните;

4.4.2. Технологично описание на регистъра

4.4.2.1. Носители на данни

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

4.4.2.2. Технология на обработване

Данните в регистър „Родители“ се събират и обработват при спазване на принципа „Необходимост да се знае“, като част от информацията се предоставя на учителите / и чрез дневниците на паралелките/ за изпълнение на служебните им задължения и за евентуална реакция при нужда. Съгласно Наредба № 8 от 11.08.2016 г. за информацията и документите за системата на предучилищното и училищното образование същите периодично се изпращат в Управленската информационна система на образованието.

Помещенията, в които се обработва и съхранява регистърът са с ограничен достъп, оборудвани са 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.

4.4.2.3. Срок на съхранение

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

4.4.2.4. Предоставени услуги

12 СУ не обработва личните данни от регистър „Родители“ за други цели, извън посочените в т. 4.4.1.1.

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

4.4.3.1. Данните в регистър „Родители“ се събират, обработват и съхраняват при спазване на принципа „Необходимост да се знае“ от лица – служители на 12 СУ:

- ЗАС;
- секретар;
- учители;
- заместник - директори;
- директор на 12 СУ.

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

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 – име, презиме, фамилия, адрес на практиката, телефон.

3.6.1.5. **Източници, от които се събират данните:**

- физически лица – родители или настойници на учащи в 12 СУ, които предоставят данни за личните лекари на учащите се в 12 СУ.

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

12 СУ 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 12 СУ:

- заместник-директори;
- учители;
- медицинска сестра.

4.6. РЕГИСТЪР „ПРОПУСКАТЕЛЕН РЕЖИМ“

4.6.1. Общо описание на регистъра

4.6.1.1. Цели на обработване на личните данни: опазване на обществения ред в сградата на 12 СУ.

4.6.1.2. Нормативно основание: Закон за частната охранителна дейност, Правилник за пропускателния режим в 12 СУ.

4.6.1.3. Категории физически лица, за които се обработват данните: учители, служители, учащи се, 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 и обработват на хартиен носител.

Помещенията, в които се събират, обработват и съхраняват са с ограничен достъп, с постоянно видеонаблюдение и физическа охрана.

4.6.2.2. Технология на обработване

Данните се предоставят от физическите лица-посетители при влизане в сградата на 12 СУ, преди изпълнение на договори.

4.6.2.3. Срок на съхранение

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

4.6.2.4. Предоставени услуги

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

4.6.3. Длъжности, свързани с обработването и защитата на лични данни от регистър „Пропускателен режим“, права и задължения

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 дежурния охранител от фирма „Егида – София” ЕАД.

4.7. РЕГИСТЪР „ВИДЕОНАБЛЮДЕНИЕ“

4.7.1. Общо описание на регистъра

4.7.1.1. Цели на обработване на лични данни:обществен ред и охранителна дейност.

4.7.1.2. Нормативно основание: Закон за частната охранителна дейност.

4.7.1.3. Категории физически лица, за които се обработват данните: служители на 12 СУ, учащи се, лица, изпълнители по сключени договори с 12 СУ, родители, посетители.

4.7.1.4. Категории лични данни: Видеоматериал.

4.7.1.5. **Източници, от които се събират данните:**

- от физическите лица, за които се отнасят данните. Зоните, в които се води видеонаблюдението са обозначени с табели.

4.7.2. Технологично описание на регистъра

4.7.2.1. Носители на данни

Данните в регистър „Видеонаблюдение" се обработват в електронен вид.

4.7.2.2. Технология на обработване

Данните в регистър „Видеонаблюдение“ се обработват електронно с помощта на камери за видеонаблюдение и компютърна техника.

4.7.2.3. Срок на съхранение

Данните в регистър „Видеонаблюдение“ се съхраняват до 30 дни.

4.7.2.4. **Предоставени услуги**

12 СУ не обработва личните данни от регистър „Видеонаблюдение“ за други цели, извън посочените в т. 4.7.1.1.

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

4.7.3.1. Данните от регистър „Видеонаблюдение“ се събират, обработват и съхраняват при спазване на принципа „Необходимост да се знае“ от директора на 12 СУ, дежурния портиер и дежурния охранител от фирма „Егида – София” ЕАД.

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

Форми на водене на регистрите

Чл. 5. (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 картотечни шкафове канцелариите на ЗАС, секретар, директор, заместник-директор;

(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 изолирани компютри, като достъпът е защитен със пароли;

2. Местонахождение на компютрите – в канцелариите на училището;

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. 6. (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. 7. 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. 8. Архивиране на личните данни се извършва периодично съгласно нормативната уредба в страната от обработващия лични данни с оглед запазване на информацията за съответните лица в актуален вид.

Контрол при обработване на личните данни

Чл. 9. Контролът върху дейностите по обработка на лични данни се осъществява от директора и заместник-директорите.

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 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 12. Средно училище „Цар Иван Асен II“;

(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.

Глава четвърта

IV. ДОСТЪП ДО ЛИЧНИ ДАННИ

Осигуряване на достъп на лицата до личните им данни

Чл. 11. (1) Всяко физическо лице, както и служителите в 12. Средно училище „Цар Иван Асен II“ 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. 12. (1) Правото на достъп се осъществява с писмена молба до администратора на лични данни. Молбата може да бъде отправена и по електронен път по реда на Закона за електронния документ и електронния подпис.

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

Чл. 13. (1) Молбата по чл. 12 съдържа:

1. трите имена, ЕГН/ЛНЧ/, адрес за контакт и телефон на заявителя;

2. описание на искането;

4. предпочитана форма за предоставяне на достъп до личните данни;

5. 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. 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 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. 15. (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. 16. Право на достъп до данните в поддържаните от администратора регистри на лични данни имат служителите в 12. СУ – 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 12. СУ с оторизиран достъпдо 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.

V. ДОСТЪП НА ТРЕТИ ЛИЦА ДО РЕГИСТРИТЕ СЪДЪРЖАЩИ ЛИЧНИ ДАННИ

Чл. 18. (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 ПЕТА

ВИДОВЕ ЗАЩИТА НА ЛИЧНИ ДАННИ

VI. ЛИЦЕ ПО ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

Чл. 19. (1) За обезпечаване на адекватна защита на регистрите с лични данни администраторът определя лице по защита на личните данни.

(2) Лицето 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 12. СУ „Цар Иван Асен II”;

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. 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) 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[1] чрез употребата на технически и организационни мерки.

6. Мерките на различните видове защита се определят съгласно заповед на директора на 12. СУ и са неразделна част от настоящите Правила.

Чл. 21 (1) Всяко лице желаещо да внесе документ съдържащ лични данни предоставя същия в деловодството на 12. СУ. Лицето приемащо документа е задължено да запознае вносителят на документите с правата му на субект на лични данни, както и с Вътрешните правила за тяхната обработка. Преди приемането му, вносителят попълва съответна Декларация по образец предоставена му от лицето приемащо документите за деклариране на предоставените лични данни и основанието, на което те се предоставят и ще се ползват. Лицето, приемащо документите има право да изиска от субекта на лични данни документа, доказващ истинността на предоставените лични данни, а при наличие на предвидена в закона възможност, да снима копие от този документ и да го приложи към декларацията.

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

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

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

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

VII. Мерки за защита при обработване на личните данни

Чл. 22. (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. 23. (1) Служителите, обработващи лични данни, вземат мерки за гарантиране на надеждност при обработването, като осъществяват 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 шеста

ОЦЕНКА НА ВЪЗДЕЙСТВИЕТО ВЪРХУ ОБРАБОТВАНИТЕ ЛИЧНИ ДАННИ

Чл. 24. (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. 25. 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.

VIII. НИВА НА ВЪЗДЕЙСТВИЕ

Чл. 26. 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. 27. (1) Администраторът извършва оценка на въздействие за всички поддържани регистри .

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

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

Чл. 28. В зависимост от нивото на въздействие се определя и съответно ниво на защита.

Чл. 29. (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 СЕДМА

IX. 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 загуба на лични данни, незабавно се докладва на лицето по защита на личните данни в 12. СУ.

(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.

X. ОТГОВОРНОСТ

Чл. 31. 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 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 12. СУ, 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.

Настоящите правила са утвърдени със заповед 970 на 28.05.2018 година.

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