**УТВЪРЖДАВАМ:**

**Виолета Жекова**

**ИНСТРУКЦИЯ**

**за мерките за защита на личните данни**

**в ЧАСТНА ДЕТСКА ГРАДИНА”ВЪЛШЕБСТВО”**

**13.05.2019г.**

**А. ЧАСТНА ДЕТСКА ГРАДИНА”ВЪЛШЕБСТВО” КАТО АДМИНИСТРАТОР НА ЛИЧНИ ДАННИ**

**І. Общи положения**

*Предмет*

**Чл. 1.** Тази инструкция урежда условията и реда за водене на регистри на лични данни, минималното ниво на технически и организационни мерки за тяхната защита, както и упражняването на контрол при обработването на лични данни в **ЧАСТНА ДЕТСКА ГРАДИНА”ВЪЛШЕБСТВО”**

*Принципи при обработване на лични данни*

**Чл. 2.** При обработването на лични данни в **ЧАСТНА ДЕТСКА ГРАДИНА”ВЪЛШЕБСТВО”**

се спазват следните принципи:

1. законосъобразност, добросъвестност и прозрачност;

2. ограничение на целите;

3. свеждане на данните до минимум;

4. точност;

5. ограничение на съхранението;

6. цялостност и поверителност;

7. отчетност.

**ІІ. Администратор и регистри с лични данни**

*Индивидуализиране на администратора на лични данни*

**Чл. 3.** (1) Администратор на лични данни е **ЧАСТНА ДЕТСКА ГРАДИНА”ВЪЛШЕБСТВО”**

със седалище и адрес на управление: гр. Пловдив, ул. Росини №1. Адресът за кореспонденция и контакт е гр. Пловдив, ул. Росини №1, тел. 0878228364

(2) Администраторът обработва лични данни във връзка с дейността си и сключването на трудови договори с родители, работници и служители, като определя сам целите и средствата за обработването им, при спазване на относимите нормативни актове.

(3) Личните данни се обработват самостоятелно от администратора на лични данни и чрез възлагане на обработващи лични данни.

(4) Администраторът може да определи едно или повече лица, които да отговарят за координиране и прилагане на мерките за защита на личните данни.

*Условия за достъп до лични данни*

**Чл. 4.** Достъпът до лични данни се осъществява само от лица, чиито служебни задължения или конкретно възложена задача налагат такъв достъп, при спазване на принципа „Необходимост да знае” и след запознаване с нормативната уредба в областта на защитата на личните данни, политиката и ръководствата за защита на личните данни и опасностите за личните данни, обработвани от администратора, като за целта лицата подписват декларация за неразгласяване на лични данни, до които са получили достъп при и по повод изпълнение на задълженията си.

*Права на физическите лица при обработване на отнасящи се за тях лични данни*

**Чл. 5.** (1) Всяко физическо лице, чийто лични данни ще се обработват от администратора, следва да бъде уведомено за:

1. данните, които идентифицират администратора;

2. целите на обработването на личните данни и правното основание за обработването;

3. категориите лични данни, отнасящи се до съответното физическо лице;

4. получателите или категориите получатели, на които могат да бъдат разкрити данните;

5. срока за съхранение на личните данни;

6. информация за правото на достъп и правото на коригиране, изтриване или ограничаване на обработването на събраните данни, правото на възражение и правото на преносимост при условията на Регламент (ЕС) 2016/679 – Общия регламент относно защитата на данните;

7. право на оттегляне на съгласието по всяко време, когато обработването на личните данни се основава на съгласие на лицето;

8. правото на жалба до надзорен орган – за Република България Комисията за защита на личните данни;

9. източника на данните;

10. съществуване на автоматизирано вземане на решения, включително профилиране.

(2) Алинея 2 не се прилага, когато:

1. обработването е за статистически, исторически или научни цели и предоставянето на данните по ал. 1 е невъзможно или изисква прекомерни усилия;

2. вписването или разкриването на данни са изрично предвидени в закон;

3. физическото лице, за което се отнасят данните, вече разполага с информацията по ал. 1;

4. е налице изрична забрана за това в закон.

*Поддържани регистри на лични данни*

**Чл. 6.** В **ЧАСТНА ДЕТСКА ГРАДИНА”ВЪЛШЕБСТВО”**

се обработват лични данни в следните регистри:

1. Регистър „Персонал“
2. Регистър „Родители/деца”
3. Регистър „Видеонаблюдение“

**ІІІ. Регистър „Персонал“**

*Общо описание на регистъра*

**Чл. 7.** В регистъра се обработват лични данни на кандидатите за работа и на служителите, работниците и изпълнителите по граждански договори с оглед:

1. индивидуализиране на трудови, служебни и граждански правоотношения;

2. изпълнение на нормативните изисквания на Кодекса на труда, Кодекса за социално осигуряване, Закона за счетоводството, Закона за данъците върху доходите на физическите лица, Закона за Националния архивен фонд и др.;

3. използване на събраните данни за съответните лица за служебни цели:

а) за всички дейности, свързани със съществуване, изменение и прекратяване на трудовите и граждански правоотношения;

б) за изготвяне на всякакви документи на лицата в тази връзка (договори, допълнителни споразумения, документи, удостоверяващи трудов стаж, служебни бележки, справки, удостоверения и др. подобни);

в) за установяване на връзка с лицето по телефон, за изпращане на кореспонденция, отнасяща се до изпълнение на задълженията му по трудови или граждански договори;

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

*Категории лични данни, обработвани в регистъра*

**Чл. 8.** В регистъра се обработват следните категории лични данни:

1. физическа идентичност: имена и паспортни данни (ЕГН, номер на лична карта, дата и място на издаване, адрес, месторождение, телефони за връзка и др.);

2. социална идентичност: данни относно образование и допълнителни квалификации (вид на образованието, място, номер и дата на издаване на дипломата), както и трудова дейност и професионална биография;

3. семейна идентичност: данни относно семейното положение на физическото лице (наличие на брак, развод, брой членове на семейството, в това число деца до 18 години);

4. икономическа идентичност: данни относно имотното и финансово състояние на физическото лице, участието и/или притежаването на дялове или ценни книжа на дружества и др.;

5. лични данни относно гражданскоправния статус на лицата, необходими за длъжностите, свързани с материална отговорност (напр. свидетелства за съдимост);

6. данни за здравословното състояние (медицинско свидетелство при постъпване на работа, периодични прегледи, преминавани с оглед характера на работата, изпълнявана по трудовото правоотношение и изискванията за безопасни условия на труд);

7. данни за членство в синдикални организации.

*Технологично описание на регистъра*

**Чл. 9.** (1) Технологичното описание на регистъра обхваща носителите на данни, технологията на обработване, срока за съхраняване и предоставяните услуги по регистъра.

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

(3) Данните в регистъра се предоставят от физическите лица при кандидатстване за работа в **ЧАСТНА ДЕТСКА ГРАДИНА”ВЪЛШЕБСТВО”**

Данните се въвеждат директно в договори, допълнителни споразумения, документи, удостоверяващи трудов стаж, служебни бележки, справки, удостоверения, кореспонденция и др.

(4) Данните в регистъра се съхраняват за срок от 50 години във връзка с нормативно установени срокове.

(5) Администраторът на лични данни предоставя достъп, справки, извлечения, издаване на документи и други услуги от съответния регистър с лични данни.

*Длъжности, свързани с обработването и защитата на лични данни от регистъра и описание на техните права и задължения*

**Чл. 10.** (1) Данните от регистъра се обработват от Виолета Жекова, директор в **ЧАСТНА ДЕТСКА ГРАДИНА”ВЪЛШЕБСТВО”**

при спазване на принципа „Необходимост да се знае”.

(2) Длъжностните лица нямат право да разпространяват информация за личните данни, станали им известни при изпълнение на служебните им задължения.

*Оценка на въздействието на Регистър Персонал“*

**Чл. 11.** (1) Оценка на въздействието на Регистър „Персонал“ се извършва в съответствие с критериите по чл. 11, ал. 2 във връзка с чл. 14 от Наредба № 1 от 30 януари 2013 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни, при съобразяване със следните обстоятелства:

1. в регистъра се обработват лични данни за лица, чийто брой надхвърля 5, но не надхвърля 10;

2. в регистъра се обработват специални категории лични данни, свързани със здравословното състояние на работниците и служителите и данни за членство в синдикални организации с оглед прилагане на изискванията на трудовото законодателство.

(2) При отчитане на критериите по ал. 1, нивото на въздействие на Регистър „Персонал“ е средно.

(3) 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.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Оценка на нивото на въздействие на „Регистъра на служителите“ | | | | |
| **Наименование на**  **регистъра** | **НИВО НА ВЪЗДЕЙСТВИЕ** | | | |
| **поверителност** | **цялостност** | **наличност** | **общо за регистъра** |
| Персонал | средно | средно | средно | средно |

*Технически и организационни мерки за защита на личните данни в Регистър „Персонал“*

Съгласно условията на Регламент (ЕС) 2016/679 – Общия регламент относно защитата на данните: ”като се имат предвид достиженията на техническия прогрес, разходите за прилагане и естеството, обхватът, контекстът и целите на обработването, както и рисковете с различна вероятност и тежест за правата и свободите на физическите лица, администраторът и обработващият лични данни прилагат подходящи технически и организационни мерки за осигуряване на съобразено с този риск ниво на сигурност, включително, *inter alia/наред с другите неща/*, когато е целесъобразно:

a) псевдонимизация и криптиране на личните данни; 4.5.2016 г. L 119/51 Официален вестник на Европейския съюз BG

б) способност за гарантиране на постоянна поверителност, цялостност, наличност и устойчивост на системите и услугите за обработване;

в) способност за своевременно възстановяване на наличността и достъпа до личните данни в случай на физически или технически инцидент;

г) процес на редовно изпитване, преценяване и оценка на ефективността на техническите и организационните мерки с оглед да се гарантира сигурността на обработването.

….При оценката на подходящото ниво на сигурност се вземат предвид по-специално рисковете, които са свързани с обработването, по-специално от случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или достъп до прехвърлени, съхранявани или обработени по друг начин лични данни.”

В съзвучие с тази разпоредба на Регламента се разработват, утвърждават и внедряват мерките за физическа, документална, персонална защита и защита на информационните масиви от бази данни. Мерките се определят така, че да гарантират избягване на оценените рискове, да гарантират спазването на принципите при обработката на личните данни, но и да не създават допълнителни пречки при обработката на данните, които биха били затрудняващи фактори, но не биха допринесли за повишаване на сигурността на защитата на данните и не биха били допълнителна гаранция за спазване на принципите на обработка на личните данни.

**Чл. 12.** (1) Физическата защита на личните данни се осъществява при спазване на следните мерки:

1. Личните данни от регистъра се обработват в кабинетите на упълномощените по чл. 10 лица.

2. Всички документи на хартиен носител, съдържащи лични данни, се съхраняват в определени шкафове в кабинети, а достъпът до тях е ограничен само за упълномощени лица.

3. Елементите на комуникационно-информационните системи, използвани за обработване на лични данни се намират в шкаф, в помещение със зони, определени за тяхното съхранение.

4. Помещенията, в които се обработват лични данни от регистъра, са оборудвани със заключване на вратите и пожарогасителни средства.

5. Физическият достъп до зоните в обекта с ограничен достъп, включително и тези, в които са разположени елементи на комуникационно-информационните системи, е възможен само през заключващи се врати. Достъп се предоставя само на служителите, чийто служебни задължения включват обработване на лични данни от регистъра.

6. Външни лица имат достъп до помещенията, в които се обработват лични данни от регистъра, само в присъствието на упълномощени служители, но тези лица нямат достъп до шкафовете, в които се съхраняват личните данни. Целият офис на **ЧАСТНА ДЕТСКА ГРАДИНА”ВЪЛШЕБСТВО”** предвид естеството на основната дейност на администратора- извършване на счетоводни услуги, представлява помещение, което се достъпва единствено от лица, които са в трудово правни отношения с администратора и са упълномощени да боравят с данните, съхранявани в него. Посещенията от външни лица се осъществява в приемна, отделена от зоните, в които се съхраняват документи, съдържащи лични данни под каквато и да било форма.

(2) Персоналната защита на личните данни се осъществява при спазване на следните мерки:

1. Лицата, обработващи лични данни, се запознават със ЗЗЛД, Наредба № 1 от 30 януари 2013 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни, настоящата Инструкция и правилата за информационна сигурност при постъпване на работа.

2. Лицата, обработващи лични данни, преминават обучение, включващо запознаване с политиката и ръководствата за защита на личните данни, запознаване с опасностите за личните данни, обработвани от администратора, като се провежда тренировка на персонала за реакция при събития, застрашаващи сигурността на данните.

3. Лицата, обработващи лични данни, задължително подписват декларация, с която поемат задължение за неразпространение на лични данни станали им известни във връзка и по време на изпълнение на служебните им задължения. Декларацията се съхранява в кадровото досие на всеки служител.

4. Споделяне на критична информация между служителите (като идентификатори, пароли за достъп и т.н.) е забранено от политиките за информационна сигурност.

(3) Документалната защита на обработваните в регистъра лични данни се осъществява при спазване на следните мерки:

1. Регистър „Персонал“ се поддържа на хартиен носител (кадрови досиета, чието съдържание съответства на нормативната уредба на Република България, както и на вътрешните нужди за периодична оценка на служителите), а отделни дейности по обработване на данните в него налагат поддържане на данни в електронен вид.

2. Обработването на личните данни се извършва в рамките на работното време на **ЧАСТНА ДЕТСКА ГРАДИНА”ВЪЛШЕБСТВО”**

3. Достъп до регистъра имат лицата по чл. 10 в съответствие с принципа „Необходимост да се знае”.

4. Личните данни се събират само с конкретна цел, в съответствие с нормативните изисквания към администратора. Данните се класифицират в съответствие с тяхното предназначение и характер и се съхраняват в заключващ се шкаф в зоните с ограничен достъп.

5. Виолета Гинова Жекова е отговорна за контрол на достъпа до регистъра.

6. Сроковете за съхранение на документи от Регистър „Персонал“, които са на хартиен носител, са определени в чл. 9, ал. 4.

7. Документите се съхраняват в отредените за целта служебни помещения в **ЧАСТНА ДЕТСКА ГРАДИНА”ВЪЛШЕБСТВО”.**

8. Архивирането на документи се възлага на Виолета Гинова Жекова при спазване на съответните защитни мерки за определеното ниво на защита.

9. Личните данни могат да бъдат размножавани и разпространявани от упълномощените служители само ако е необходимо за изпълнение на служебни задължения или ако са изискани по надлежния ред от държавни органи или упълномощени лица.

10. Временните документи от регистъра, които са на хартиен носител и съдържат лични данни, се унищожават само чрез специално устройство (шредер).

11. След изтичане на срока за съхранение документите от регистъра се унищожават чрез нарязване или изгаряне, за което се съставя протокол от Виолета Гинова Жекова.

(4) Защитата на автоматизирани информационни системи и мрежи се осъществява при спазване на следните мерки:

1. При работа с данните от регистъра се използват съответните софтуерни продукти за обработване. Данните се въвеждат в база данни и се съхраняват на сървър. Всеки упълномощен служител има личен профил (потребителско име и парола), с определени съобразно задълженията му права и нива на достъп. Дефинирани са и уникални потребителски имена и пароли за стартиране на операционната система на всеки един компютър.

2. Администраторът създава и поддържа стандартни и сигурни конфигурации за всяка компютърна и мрежова платформа, с която оперира, което включва стандартни и базови конфигурации за защита на операционната система, защитни стени, рутери и мрежови устройства. За защита на данните е инсталирана антивирусна програма и се извършва периодична профилактика на софтуера и системните файлове.

3.Директорът Виолета Гинова Жекова е отговорна за управлението на регистъра. Само лицата посочени в чл. 10 имат достъп до регистъра.

4. За всички компютърни конфигурации, сървъри и комуникационни средства, от които зависи правилното поддържане на базите данни, са осигурени непрекъсваеми токозахранващи устройства (UPS).

5. В помещенията, в които са разположени компютърни и комуникационни средства, е осигурено заключване на помещенията, сигнално-охранителна система.

6.Допълнителни копия на носителите на информация, съдържащи лични данни, се съхраняват на сървър.

7. Контролът по използването на тези носители се осъществява от Виолета Гинова Жекова.

8. Организационни мерки за гарантиране нивото на сигурност:

а) Охрана на сградата с денонощна охрана, осъществявана от специализирано предприятие, извършващо охранителни услуги.

б) Забранено е използването на преносими лични носители на данни.

в) Работните компютърни конфигурации, както и цялата IT инфраструктура, включително и достъпът до интернет, се използват единствено за служебни цели.

г) При ремонт на компютърна техника, на която се съхраняват лични данни, предоставянето й на сервизната организация се извършва без устройствата, на които се съхраняват лични данни.

9. Не се разрешава осъществяването на отдалечен достъп до данни от регистъра.

10. Сроковете за съхранение на данни от регистъра са описани в чл. 9, ал. 4.

(5) Криптографската защита при предаване на данни по електронен път или на преносими технически носители се осъществява чрез използване на стандартни технологии за криптиране на данните, както и използване на електронен подпис.

*Действия за защита при аварии, произшествия и бедствия*

**Чл. 13.** (1) При възникване и установяване на инцидент, веднага се докладва на лицето, отговорно за защитата на личните данни.

(2) За инцидентите се води дневник, в който задължително се вписват предполагаемото време или период на възникване, времето на установяване, времето на докладване и името на служителя, извършил доклада. След анализ на инцидента, упълномощено лице вписва в дневника последствията от инцидента и мерките, които са предприети за отстраняването им.

(3) В случаите на необходимост от възстановяване на данни, процедурата се изпълнява от Виолета Гинова Жекова , като това се отразява в дневника по архивиране и възстановяване на данни.

*Предоставяне на лични данни на трети лица*

**Чл. 14.** (1) Данни от регистъра могат да бъдат предоставяни на държавни институции с оглед изпълнение на нормативно задължение (НОИ, НАП, МВР и т.н.).

(2) В качеството си на работодател, **ЧАСТНА ДЕТСКА ГРАДИНА”ВЪЛШЕБСТВО”**

предоставя лични данни и на определени кредитни институции (банки) във връзка с изплащането на дължимите възнаграждения на служители и изпълнители по граждански договори. Личните данни, който се предоставят, са три имена и единен граждански номер и се предоставят с цел идентификация на лицето, в чиято полза се извършва плащането. Това се налага, с оглед изискванията на кредитните институции във връзка с извършваните от тях банкови преводи.

(3) Във връзка с използването на куриерски услуги – приемане, пренасяне и доставка и адресиране на пратките до физически лица **ЧАСТНА ДЕТСКА ГРАДИНА”ВЪЛШЕБСТВО”**

посочва следните данни: три имена, адрес, област, пощенски код и наименование на населеното място.

*Срок за провеждане на периодични прегледи относно необходимостта от обработване/заличаване на данните*

**Чл. 15.** **ЧАСТНА ДЕТСКА ГРАДИНА”ВЪЛШЕБСТВО”**

трябва да извършва ежегодни проверки на личните данни от регистъра с оглед преценка на необходимостта от тяхното обработване и съответно ако е отпаднало задължението – за заличаването им.

*Ред за изпълнение на задълженията по чл. 25 от ЗЗЛД*

**Чл. 16.** (1)След изтичане на срока за съхранение на данните, комисия определя кои документи подлежат на унищожение и мястото на извършване на процедурата.

(2) Унищожението се извършва посредством няколко начина, определени в зависимост от наличните към момента на унищожението технически възможности за **ЧАСТНА ДЕТСКА ГРАДИНА”ВЪЛШЕБСТВО”** , а именно: чрез разрязване с помощта на машина – шредер и/или чрез изгаряне или разрушаване (отваряне) на корпуса на носителя на данни.

(3) В случай на прехвърляне на данните на друг администратор е необходимо да се уведоми КЗЛД, ако прехвърлянето е предвидено в закон и е налице идентичност на целите на обработването и се съставят съответно приемо-предавателни протоколи.

**ІІІ. Регистър „Родители/деца“**

*Общо описание на регистъра*

**Чл. 17.** В регистъра се обработват лични данни на родители и деца във връзка с договор за обучение и образование на децата.

1. изпълнение на нормативните изисквания на закона за образованието;

3. използване на събраните данни за съответните лица за служебни цели:

б) за изготвяне на всякакви документи на лицата в тази връзка (договори, допълнителни споразумения, служебни бележки, справки, удостоверения и др. подобни);

в) за установяване на връзка с лицето по телефон, за изпращане на кореспонденция;

г) за водене на счетоводна отчетност;

*Категории лични данни, обработвани в регистъра*

**Чл. 18.** В регистъра се обработват следните категории лични данни:

1. физическа идентичност: имена и паспортни данни (ЕГН, номер на лична карта, дата и място на издаване, адрес, месторождение, телефони за връзка и др.);

2. социална идентичност: данни относно образование и допълнителни квалификации (вид на образованието, място, номер и дата на издаване на дипломата), както и трудова дейност и професионална биография;

3. семейна идентичност: данни относно семейното положение на физическото лице (наличие на брак, развод, брой членове на семейството, в това число деца до 18 години);

4. данни за здравословното състояние (медицински изледвания на родители и деца);

*Технологично описание на регистъра*

**Чл. 19.** (1) Технологичното описание на регистъра обхваща носителите на данни, технологията на обработване, срока за съхраняване и предоставяните услуги по регистъра.

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

(3) Данните в регистъра се предоставят от физическите лица при кандидатстване за работа в **ЧАСТНА ДЕТСКА ГРАДИНА”ВЪЛШЕБСТВО”**

Данните се въвеждат директно в договори, допълнителни споразумения, документи, удостоверяващи трудов стаж, служебни бележки, справки, удостоверения, кореспонденция и др.

(4) Данните в регистъра се съхраняват за срок от 50 години във връзка с нормативно установени срокове.

(5) Администраторът на лични данни предоставя достъп, справки, извлечения, издаване на документи и други услуги от съответния регистър с лични данни.

*Длъжности, свързани с обработването и защитата на лични данни от регистъра и описание на техните права и задължения*

**Чл. 20.** (1) Данните от регистъра се обработват от Виолета Жекова, директор в **ЧАСТНА ДЕТСКА ГРАДИНА”ВЪЛШЕБСТВО”**

при спазване на принципа „Необходимост да се знае”.

(2) Длъжностните лица нямат право да разпространяват информация за личните данни, станали им известни при изпълнение на служебните им задължения.

*Оценка на въздействието на Регистър „Родители/деца“*

**Чл. 21.** (1) Оценка на въздействието на Регистър „Родители/деца“ се извършва в съответствие с критериите по чл. 11, ал. 2 във връзка с чл. 14 от Наредба № 1 от 30 януари 2013 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни, при съобразяване със следните обстоятелства:

1. в регистъра се обработват лични данни за лица, чийто брой надхвърля 5, но не надхвърля 10;

2. в регистъра се обработват специални категории лични данни, свързани със здравословното състояние на работниците и служителите и данни за членство в синдикални организации с оглед прилагане на изискванията на трудовото законодателство.

(2) При отчитане на критериите по ал. 1, нивото на въздействие на Регистър „Родители/деца“ е средно.

(3) 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.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Оценка на нивото на въздействие на „Регистъра на родители/деца“ | | | | |
| **Наименование на**  **регистъра** | **НИВО НА ВЪЗДЕЙСТВИЕ** | | | |
| **поверителност** | **цялостност** | **наличност** | **общо за регистъра** |
| Родители/деца | средно | средно | средно | средно |

*Технически и организационни мерки за защита на личните данни в Регистър „Родители/деца“*

Съгласно условията на Регламент (ЕС) 2016/679 – Общия регламент относно защитата на данните: ”като се имат предвид достиженията на техническия прогрес, разходите за прилагане и естеството, обхватът, контекстът и целите на обработването, както и рисковете с различна вероятност и тежест за правата и свободите на физическите лица, администраторът и обработващият лични данни прилагат подходящи технически и организационни мерки за осигуряване на съобразено с този риск ниво на сигурност, включително, *inter alia/наред с другите неща/*, когато е целесъобразно:

a) псевдонимизация и криптиране на личните данни; 4.5.2016 г. L 119/51 Официален вестник на Европейския съюз BG

б) способност за гарантиране на постоянна поверителност, цялостност, наличност и устойчивост на системите и услугите за обработване;

в) способност за своевременно възстановяване на наличността и достъпа до личните данни в случай на физически или технически инцидент;

г) процес на редовно изпитване, преценяване и оценка на ефективността на техническите и организационните мерки с оглед да се гарантира сигурността на обработването.

….При оценката на подходящото ниво на сигурност се вземат предвид по-специално рисковете, които са свързани с обработването, по-специално от случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или достъп до прехвърлени, съхранявани или обработени по друг начин лични данни.”

В съзвучие с тази разпоредба на Регламента се разработват, утвърждават и внедряват мерките за физическа, документална, персонална защита и защита на информационните масиви от бази данни. Мерките се определят така, че да гарантират избягване на оценените рискове, да гарантират спазването на принципите при обработката на личните данни, но и да не създават допълнителни пречки при обработката на данните, които биха били затрудняващи фактори, но не биха допринесли за повишаване на сигурността на защитата на данните и не биха били допълнителна гаранция за спазване на принципите на обработка на личните данни.

**Чл. 22.** (1) Физическата защита на личните данни се осъществява при спазване на следните мерки:

1. Личните данни от регистъра се обработват в кабинетите на упълномощените по чл. 10 лица. 2. Всички документи на хартиен носител, съдържащи лични данни, се съхраняват в определени шкафове в кабинети, а достъпът до тях е ограничен само за упълномощени лица.

3. Елементите на комуникационно-информационните системи, използвани за обработване на лични данни се намират в шкаф, в помещение със зони, определени за тяхното съхранение.

4. Помещенията, в които се обработват лични данни от регистъра, са оборудвани със заключване на вратите и пожарогасителни средства.

5. Физическият достъп до зоните в обекта с ограничен достъп, включително и тези, в които са разположени елементи на комуникационно-информационните системи, е възможен само през заключващи се врати. Достъп се предоставя само на служителите, чийто служебни задължения включват обработване на лични данни от регистъра.

6. Външни лица имат достъп до помещенията, в които се обработват лични данни от регистъра, само в присъствието на упълномощени служители, но тези лица нямат достъп до шкафовете, в които се съхраняват личните данни. Целият офис на **ЧАСТНА ДЕТСКА ГРАДИНА”ВЪЛШЕБСТВО”** предвид естеството на основната дейност на администратора- извършване на счетоводни услуги, представлява помещение, което се достъпва единствено от лица, които са в трудово правни отношения с администратора и са упълномощени да боравят с данните, съхранявани в него. Посещенията от външни лица се осъществява в приемна, отделена от зоните, в които се съхраняват документи, съдържащи лични данни под каквато и да било форма.

(2) Персоналната защита на личните данни се осъществява при спазване на следните мерки:

1. Лицата, обработващи лични данни, се запознават със ЗЗЛД, Наредба № 1 от 30 януари 2013 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни, настоящата Инструкция и правилата за информационна сигурност при постъпване на работа.

2. Лицата, обработващи лични данни, преминават обучение, включващо запознаване с политиката и ръководствата за защита на личните данни, запознаване с опасностите за личните данни, обработвани от администратора, като се провежда тренировка на персонала за реакция при събития, застрашаващи сигурността на данните.

3. Лицата, обработващи лични данни, задължително подписват декларация, с която поемат задължение за неразпространение на лични данни станали им известни във връзка и по време на изпълнение на служебните им задължения. Декларацията се съхранява в кадровото досие на всеки служител.

4. Споделяне на критична информация между служителите (като идентификатори, пароли за достъп и т.н.) е забранено от политиките за информационна сигурност.

(3) Документалната защита на обработваните в регистъра лични данни се осъществява при спазване на следните мерки:

1. Регистър „Персонал“ се поддържа на хартиен носител (кадрови досиета, чието съдържание съответства на нормативната уредба на Република България, както и на вътрешните нужди за периодична оценка на служителите), а отделни дейности по обработване на данните в него налагат поддържане на данни в електронен вид.

2. Обработването на личните данни се извършва в рамките на работното време на **ЧАСТНА ДЕТСКА ГРАДИНА”ВЪЛШЕБСТВО”**

3. Достъп до регистъра имат лицата по чл. 10 в съответствие с принципа „Необходимост да се знае”.

4. Личните данни се събират само с конкретна цел, в съответствие с нормативните изисквания към администратора. Данните се класифицират в съответствие с тяхното предназначение и характер и се съхраняват в заключващ се шкаф в зоните с ограничен достъп.

5. Виолета Гинова Жекова е отговорна за контрол на достъпа до регистъра.

6. Сроковете за съхранение на документи от Регистър „Персонал“, които са на хартиен носител, са определени в чл. 9, ал. 4.

7. Документите се съхраняват в отредените за целта служебни помещения в **ЧАСТНА ДЕТСКА ГРАДИНА”ВЪЛШЕБСТВО”.**

8. Архивирането на документи се възлага на Виолета Гинова Жекова при спазване на съответните защитни мерки за определеното ниво на защита.

9. Личните данни могат да бъдат размножавани и разпространявани от упълномощените служители само ако е необходимо за изпълнение на служебни задължения или ако са изискани по надлежния ред от държавни органи или упълномощени лица.

10. Временните документи от регистъра, които са на хартиен носител и съдържат лични данни, се унищожават само чрез специално устройство (шредер).

11. След изтичане на срока за съхранение документите от регистъра се унищожават чрез нарязване или изгаряне, за което се съставя протокол от Виолета Гинова Жекова.

(4) Защитата на автоматизирани информационни системи и мрежи се осъществява при спазване на следните мерки:

1. При работа с данните от регистъра се използват съответните софтуерни продукти за обработване. Данните се въвеждат в база данни и се съхраняват на сървър. Всеки упълномощен служител има личен профил (потребителско име и парола), с определени съобразно задълженията му права и нива на достъп. Дефинирани са и уникални потребителски имена и пароли за стартиране на операционната система на всеки един компютър.

2. Администраторът създава и поддържа стандартни и сигурни конфигурации за всяка компютърна и мрежова платформа, с която оперира, което включва стандартни и базови конфигурации за защита на операционната система, защитни стени, рутери и мрежови устройства. За защита на данните е инсталирана антивирусна програма и се извършва периодична профилактика на софтуера и системните файлове.

3.Директорът Виолета Гинова Жекова е отговорна за управлението на регистъра. Само лицата посочени в чл. 10 имат достъп до регистъра.

4. За всички компютърни конфигурации, сървъри и комуникационни средства, от които зависи правилното поддържане на базите данни, са осигурени непрекъсваеми токозахранващи устройства (UPS).

5. В помещенията, в които са разположени компютърни и комуникационни средства, е осигурено заключване на помещенията, сигнално-охранителна система.

6.Допълнителни копия на носителите на информация, съдържащи лични данни, се съхраняват на сървър.

7. Контролът по използването на тези носители се осъществява от Виолета Гинова Жекова.

8. Организационни мерки за гарантиране нивото на сигурност:

а) Охрана на сградата с денонощна охрана, осъществявана от специализирано предприятие, извършващо охранителни услуги.

б) Забранено е използването на преносими лични носители на данни.

в) Работните компютърни конфигурации, както и цялата IT инфраструктура, включително и достъпът до интернет, се използват единствено за служебни цели.

г) При ремонт на компютърна техника, на която се съхраняват лични данни, предоставянето й на сервизната организация се извършва без устройствата, на които се съхраняват лични данни.

9. Не се разрешава осъществяването на отдалечен достъп до данни от регистъра.

10. Сроковете за съхранение на данни от регистъра са описани в чл. 9, ал. 4.

(5) Криптографската защита при предаване на данни по електронен път или на преносими технически носители се осъществява чрез използване на стандартни технологии за криптиране на данните, както и използване на електронен подпис.

*Действия за защита при аварии, произшествия и бедствия*

**Чл. 23.** (1) При възникване и установяване на инцидент, веднага се докладва на лицето, отговорно за защитата на личните данни.

(2) За инцидентите се води дневник, в който задължително се вписват предполагаемото време или период на възникване, времето на установяване, времето на докладване и името на служителя, извършил доклада. След анализ на инцидента, упълномощено лице вписва в дневника последствията от инцидента и мерките, които са предприети за отстраняването им.

(3) В случаите на необходимост от възстановяване на данни, процедурата се изпълнява от Виолета Гинова Жекова , като това се отразява в дневника по архивиране и възстановяване на данни.

*Предоставяне на лични данни на трети лица*

**Чл. 24.** (1) Данни от регистъра могат да бъдат предоставяни на държавни институции с оглед изпълнение на нормативно задължение (НОИ, НАП, МВР и т.н.).

(2) В качеството си на работодател, **ЧАСТНА ДЕТСКА ГРАДИНА”ВЪЛШЕБСТВО”**

предоставя лични данни и на определени кредитни институции (банки) във връзка с изплащането на дължимите възнаграждения на служители и изпълнители по граждански договори. Личните данни, който се предоставят, са три имена и единен граждански номер и се предоставят с цел идентификация на лицето, в чиято полза се извършва плащането. Това се налага, с оглед изискванията на кредитните институции във връзка с извършваните от тях банкови преводи.

(3) Във връзка с използването на куриерски услуги – приемане, пренасяне и доставка и адресиране на пратките до физически лица **ЧАСТНА ДЕТСКА ГРАДИНА”ВЪЛШЕБСТВО”**

посочва следните данни: три имена, адрес, област, пощенски код и наименование на населеното място.

*Срок за провеждане на периодични прегледи относно необходимостта от обработване/заличаване на данните*

**Чл. 25.** **ЧАСТНА ДЕТСКА ГРАДИНА”ВЪЛШЕБСТВО”**

трябва да извършва ежегодни проверки на личните данни от регистъра с оглед преценка на необходимостта от тяхното обработване и съответно ако е отпаднало задължението – за заличаването им.

*Ред за изпълнение на задълженията по чл. 25 от ЗЗЛД*

**Чл. 26.** (1)След изтичане на срока за съхранение на данните, комисия определя кои документи подлежат на унищожение и мястото на извършване на процедурата.

(2) Унищожението се извършва посредством няколко начина, определени в зависимост от наличните към момента на унищожението технически възможности за **ЧАСТНА ДЕТСКА ГРАДИНА”ВЪЛШЕБСТВО”** , а именно: чрез разрязване с помощта на машина – шредер и/или чрез изгаряне или разрушаване (отваряне) на корпуса на носителя на данни.

(3) В случай на прехвърляне на данните на друг администратор е необходимо да се уведоми КЗЛД, ако прехвърлянето е предвидено в закон и е налице идентичност на целите на обработването и се съставят съответно приемо-предавателни протоколи.

**ІV. Регистър за „Видеонаблюдение“**

*Общо описание на регистъра*

**Чл. 27.** В регистъра се обработват лични данни на родители, деца, служители и други лица посещаващи детската градина на основание чл.4, ал.1 т.4 от ЗЗЛД

**Цели**: 1.Подобряване на сигурността и прозрачността на грижите, както и решаване на възникнали конфликти при отглеждането на децата в детското заведение.

2. Защита на живота и здравето на лицата, обект на видеонаблюдение;

3. Разкриване, предотвратяване и контрол на нарушения/престъпления;

4. Защита на собствеността.

*Категории лични данни, обработвани в регистъра*

**Чл. 28.** В регистъра се обработват следните категории лични данни:

1. физическа идентичност: запис на образи и звук.

*Технологично описание на регистъра*

**Чл. 29.** (1) Технологичното описание на регистъра обхваща носителите на данни, технологията на обработване, срока за съхраняване и предоставяните услуги по регистъра.

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

(3) Данните в регистъра се съхраняват за срок от 10 дни след което автоматично се изтриват.

*Длъжности, свързани с обработването и защитата на лични данни от регистъра и описание на техните права и задължения*

**Чл. 30.** (1) Данните от регистъра се обработват от Виолета Жекова, директор в **ЧАСТНА ДЕТСКА ГРАДИНА”ВЪЛШЕБСТВО”**

при спазване на принципа „Необходимост да се знае”.

(2) Длъжностните лица нямат право да разпространяват информация за личните данни, станали им известни при изпълнение на служебните им задължения.

*Оценка на въздействието на Регистър „Видеонаблюдение“*

**Чл. 31.** (1) Оценка на въздействието на Регистър „Видеонаблюдение“ се извършва в съответствие с критериите по чл. 11, ал. 2 във връзка с чл. 14 от Наредба № 1 от 30 януари 2013 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни, при съобразяване със следните обстоятелства:

1. в регистъра се обработват лични данни за лица, чийто брой надхвърля 10, но не надхвърля 50;

(2) При отчитане на критериите по ал. 1, нивото на въздействие на Регистър „Видеозаснемане“ е средно.

(3) 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.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Оценка на нивото на въздействие на „Регистъра на родители/деца“ | | | | |
| **Наименование на**  **регистъра** | **НИВО НА ВЪЗДЕЙСТВИЕ** | | | |
| **поверителност** | **цялостност** | **наличност** | **общо за регистъра** |
| Родители/деца | средно | средно | средно | средно |

*Технически и организационни мерки за защита на личните данни в Регистър „Видеозаснемане“*

Съгласно условията на Регламент (ЕС) 2016/679 – Общия регламент относно защитата на данните: ”като се имат предвид достиженията на техническия прогрес, разходите за прилагане и естеството, обхватът, контекстът и целите на обработването, както и рисковете с различна вероятност и тежест за правата и свободите на физическите лица, администраторът и обработващият лични данни прилагат подходящи технически и организационни мерки за осигуряване на съобразено с този риск ниво на сигурност, включително, *inter alia/наред с другите неща/*, когато е целесъобразно:

a) псевдонимизация и криптиране на личните данни; 4.5.2016 г. L 119/51 Официален вестник на Европейския съюз BG

б) способност за гарантиране на постоянна поверителност, цялостност, наличност и устойчивост на системите и услугите за обработване;

в) способност за своевременно възстановяване на наличността и достъпа до личните данни в случай на физически или технически инцидент;

г) процес на редовно изпитване, преценяване и оценка на ефективността на техническите и организационните мерки с оглед да се гарантира сигурността на обработването.

….При оценката на подходящото ниво на сигурност се вземат предвид по-специално рисковете, които са свързани с обработването, по-специално от случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или достъп до прехвърлени, съхранявани или обработени по друг начин лични данни.”

В съзвучие с тази разпоредба на Регламента се разработват, утвърждават и внедряват мерките за физическа, документална, персонална защита и защита на информационните масиви от бази данни. Мерките се определят така, че да гарантират избягване на оценените рискове, да гарантират спазването на принципите при обработката на личните данни, но и да не създават допълнителни пречки при обработката на данните, които биха били затрудняващи фактори, но не биха допринесли за повишаване на сигурността на защитата на данните и не биха били допълнителна гаранция за спазване на принципите на обработка на личните данни.

**Чл. 32.** (1) Физическата защита на личните данни се осъществява при спазване на следните мерки:

1. Личните данни от регистъра се обработват в кабинетите на упълномощените по чл. 10 лица.

2. Елементите на комуникационно-информационните системи, използвани за обработване на лични данни се намират на твърд диск в изолиран компютър, в помещение със зони, определени за тяхното съхранение.

3. Помещенията, в които се обработват лични данни от регистъра, са оборудвани със заключване на вратите и пожарогасителни средства.

4. Физическият достъп до зоните в обекта с ограничен достъп, включително и тези, в които са разположени елементи на комуникационно-информационните системи, е възможен само през заключващи се врати. Достъп се предоставя само на служителите, чийто служебни задължения включват обработване на лични данни от регистъра.

5. Външни лица имат достъп до помещенията, в които се обработват лични данни от регистъра, само в присъствието на упълномощени служители, но тези лица нямат достъп до компютъра, в които се съхраняват личните данни. Целият офис на **ЧАСТНА ДЕТСКА ГРАДИНА”ВЪЛШЕБСТВО”** предвид естеството на основната дейност на администратора- извършване на административни услуги, представлява помещение, което се достъпва единствено от лица, които са в трудово правни отношения с администратора и са упълномощени да боравят с данните, съхранявани в него. Посещенията от външни лица се осъществява в приемна, отделена от зоните, в които се съхраняват документи, съдържащи лични данни под каквато и да било форма.

(2) Персоналната защита на личните данни се осъществява при спазване на следните мерки:

1. Лицата, обработващи лични данни, се запознават със ЗЗЛД, Наредба № 1 от 30 януари 2013 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни, настоящата Инструкция и правилата за информационна сигурност при постъпване на работа.

2. Лицата, обработващи лични данни, преминават обучение, включващо запознаване с политиката и ръководствата за защита на личните данни, запознаване с опасностите за личните данни, обработвани от администратора, като се провежда тренировка на персонала за реакция при събития, застрашаващи сигурността на данните.

3. Лицата, обработващи лични данни, задължително подписват декларация, с която поемат задължение за неразпространение на лични данни станали им известни във връзка и по време на изпълнение на служебните им задължения. Декларацията се съхранява в кадровото досие на всеки служител.

4. Споделяне на критична информация между служителите (като идентификатори, пароли за достъп и т.н.) е забранено от политиките за информационна сигурност.

(3) Документалната защита на обработваните в регистъра лични данни се осъществява при спазване на следните мерки:

1. Регистър „Видеонаблюдение“ се поддържа на електронен носител.

2. Обработването на личните данни се извършва в рамките на работното време на **ЧАСТНА ДЕТСКА ГРАДИНА”ВЪЛШЕБСТВО”**

3. Достъп до регистъра имат лицата по чл. 10 в съответствие с принципа „Необходимост да се знае”.

4. Личните данни се събират само с конкретна цел, в съответствие с нормативните изисквания към администратора. Данните се класифицират в съответствие с тяхното предназначение и характер и се съхраняват в заключващ се шкаф в зоните с ограничен достъп.

5. Виолета Гинова Жекова е отговорна за контрол на достъпа до регистъра.

6. Сроковете за съхранение на документи от Регистър „Видеонаблюдение“, които са на електронен носител, са определени в чл. 9, ал. 4.

7. Документите се съхраняват в отредените за целта служебни помещения в **ЧАСТНА ДЕТСКА ГРАДИНА”ВЪЛШЕБСТВО”.**

8. Архивирането на документи се възлага на Виолета Гинова Жекова при спазване на съответните защитни мерки за определеното ниво на защита.

9. Личните данни могат да бъдат размножавани и разпространявани от упълномощените служители само ако е необходимо за изпълнение на служебни задължения или ако са изискани по надлежния ред от държавни органи или упълномощени лица.

10. Временните документи от регистъра, които са на хартиен носител и съдържат лични данни, се унищожават само чрез специално устройство (шредер).

11. След изтичане на срока за съхранение документите от регистъра се унищожават чрез нарязване или изгаряне, за което се съставя протокол от Виолета Гинова Жекова.

(4) Защитата на автоматизирани информационни системи и мрежи се осъществява при спазване на следните мерки:

1. При работа с данните от регистъра се използват съответните софтуерни продукти за обработване. Данните се въвеждат в база данни и се съхраняват на сървър. Всеки упълномощен служител има личен профил (потребителско име и парола), с определени съобразно задълженията му права и нива на достъп. Дефинирани са и уникални потребителски имена и пароли за стартиране на операционната система на всеки един компютър.

2. Администраторът създава и поддържа стандартни и сигурни конфигурации за всяка компютърна и мрежова платформа, с която оперира, което включва стандартни и базови конфигурации за защита на операционната система, защитни стени, рутери и мрежови устройства. За защита на данните е инсталирана антивирусна програма и се извършва периодична профилактика на софтуера и системните файлове.

3.Директорът Виолета Гинова Жекова е отговорна за управлението на регистъра. Само лицата посочени в чл. 10 имат достъп до регистъра.

4. За всички компютърни конфигурации, сървъри и комуникационни средства, от които зависи правилното поддържане на базите данни, са осигурени непрекъсваеми токозахранващи устройства (UPS).

5. В помещенията, в които са разположени компютърни и комуникационни средства, е осигурено заключване на помещенията, сигнално-охранителна система.

6.Допълнителни копия на носителите на информация, съдържащи лични данни, се съхраняват на сървър.

7. Контролът по използването на тези носители се осъществява от Виолета Гинова Жекова.

8. Организационни мерки за гарантиране нивото на сигурност:

а) Охрана на сградата с денонощна охрана, осъществявана от специализирано предприятие, извършващо охранителни услуги.

б) Забранено е използването на преносими лични носители на данни.

в) Работните компютърни конфигурации, както и цялата IT инфраструктура, включително и достъпът до интернет, се използват единствено за служебни цели.

г) При ремонт на компютърна техника, на която се съхраняват лични данни, предоставянето й на сервизната организация се извършва без устройствата, на които се съхраняват лични данни.

9. Не се разрешава осъществяването на отдалечен достъп до данни от регистъра.

10. Сроковете за съхранение на данни от регистъра са описани в чл. 9, ал. 4.

(5) Криптографската защита при предаване на данни по електронен път или на преносими технически носители се осъществява чрез използване на стандартни технологии за криптиране на данните, както и използване на електронен подпис.

*Действия за защита при аварии, произшествия и бедствия*

**Чл. 33.** (1) При възникване и установяване на инцидент, веднага се докладва на лицето, отговорно за защитата на личните данни.

(2) За инцидентите се води дневник, в който задължително се вписват предполагаемото време или период на възникване, времето на установяване, времето на докладване и името на служителя, извършил доклада. След анализ на инцидента, упълномощено лице вписва в дневника последствията от инцидента и мерките, които са предприети за отстраняването им.

(3) В случаите на необходимост от възстановяване на данни, процедурата се изпълнява от Виолета Гинова Жекова , като това се отразява в дневника по архивиране и възстановяване на данни.

*Предоставяне на лични данни на трети лица*

**Чл. 34.** (1) Данни от регистъра могат да бъдат предоставяни на държавни институции с оглед изпълнение на нормативно задължение (НОИ, НАП, МВР и т.н.).

(2) В качеството си на работодател, **ЧАСТНА ДЕТСКА ГРАДИНА”ВЪЛШЕБСТВО”**

предоставя лични данни и на определени кредитни институции (банки) във връзка с изплащането на дължимите възнаграждения на служители и изпълнители по граждански договори. Личните данни, който се предоставят, са три имена и единен граждански номер и се предоставят с цел идентификация на лицето, в чиято полза се извършва плащането. Това се налага, с оглед изискванията на кредитните институции във връзка с извършваните от тях банкови преводи.

(3) Във връзка с използването на куриерски услуги – приемане, пренасяне и доставка и адресиране на пратките до физически лица **ЧАСТНА ДЕТСКА ГРАДИНА”ВЪЛШЕБСТВО”**

посочва следните данни: три имена, адрес, област, пощенски код и наименование на населеното място.

*Срок за провеждане на периодични прегледи относно необходимостта от обработване/заличаване на данните*

**Чл. 35.** **ЧАСТНА ДЕТСКА ГРАДИНА”ВЪЛШЕБСТВО”**

трябва да извършва ежегодни проверки на личните данни от регистъра с оглед преценка на необходимостта от тяхното обработване и съответно ако е отпаднало задължението – за заличаването им.

*Ред за изпълнение на задълженията по чл. 25 от ЗЗЛД*

**Чл. 36.** (1)След изтичане на срока за съхранение на данните, те се самоунищожават.

(3) В случай на прехвърляне на данните на друг администратор е необходимо да се уведоми КЗЛД, ако прехвърлянето е предвидено в закон и е налице идентичност на целите на обработването и се съставят съответно приемо-предавателни протоколи.

**Б. ЧАСТНА ДЕТСКА ГРАДИНА”ВЪЛШЕБСТВО”**

**КАТО ОБРАБОТВАЩ ЛИЧНИТЕ ДАННИ ОТ ИМЕТО НА ДРУГИ АДМИНИСТРАТОРИ**

**І. Общи положения**

*Предмет*

**Чл. 1.** Тази инструкция урежда условията и реда за водене на регистри на лични данни, минималното ниво на технически и организационни мерки за тяхната защита, както и упражняването на контрол при обработването на лични данни в **ЧАСТНА ДЕТСКА ГРАДИНА”ВЪЛШЕБСТВО”**в качеството на дружеството на обработващ на личните данни от името на други администратори, които са възложили тази обработка по смисъла на чл.28 от Регламент (ЕС) 2016/679 – Общия регламент относно защитата на данните.

*Принципи при обработване на лични данни*

**Чл. 2.** При обработването на лични данни в **ЧАСТНА ДЕТСКА ГРАДИНА”ВЪЛШЕБСТВО”** в качеството му на обработващ на личните данни от името на други администратори, които са възложили тази обработка по смисъла на чл.28 от Регламент (ЕС) 2016/679 – Общия регламент относно защитата на данните се спазват следните принципи:

1. законосъобразност, добросъвестност и прозрачност;

2. ограничение на целите;

3. свеждане на данните до минимум;

4. точност;

5. ограничение на съхранението;

6. цялостност и поверителност;

7. отчетност.

**ІІ. Обработващ регистри с лични данни**

*Индивидуализиране на администратора на лични данни*

**Чл. 3.** (1) Обработващ на лични данни е **ЧАСТНА ДЕТСКА ГРАДИНА”ВЪЛШЕБСТВО”** , със седалище и адрес на управление: гр. Пловдив, ул. Росини №1 за клиенти на дружеството, които са администратори на лични данни и са възложили тази обработка да се извършва от **ЧАСТНА ДЕТСКА ГРАДИНА”ВЪЛШЕБСТВО”**.

Адресът за кореспонденция и контакт е гр. Пловдив, ул. Росини №1, тел. 0878228364

(2) Обработването на лични данни се извършва във връзка с възлагането на това обработване от други администратори на лични данни/наричани по- долу възложители/, които възложители определят целите и средствата за обработването им, при спазване на относимите нормативни актове.

(3)Обработващият данни може да определи едно или повече лица, които да отговарят за координиране и прилагане на мерките за защита на личните данни, за което се уведомява администраторът- възложител.

*Условия за достъп до лични данни*

**Чл. 4.** Достъпът до лични данни се осъществява само от лица, чиито служебни задължения или конкретно възложена задача налагат такъв достъп, при спазване на принципа „Необходимост да знае” и след запознаване с нормативната уредба в областта на защитата на личните данни, политиката и ръководствата за защита на личните данни и опасностите за личните данни, обработвани от администратора, като за целта лицата подписват декларация за неразгласяване на лични данни, до които са получили достъп при и по повод изпълнение на задълженията си.

*Права на физическите лица при обработване на отнасящи се за тях лични данни*

**Чл. 5.** (1) Всяко физическо лице, чийто лични данни ще се обработват от администратора, следва да бъде уведомено за:

1. данните, които идентифицират администратора;

2. целите на обработването на личните данни и правното основание за обработването;

3. категориите лични данни, отнасящи се до съответното физическо лице;

4. получателите или категориите получатели, на които могат да бъдат разкрити данните;

5. срока за съхранение на личните данни;

6. информация за правото на достъп и правото на коригиране, изтриване или ограничаване на обработването на събраните данни, правото на възражение и правото на преносимост при условията на Регламент (ЕС) 2016/679 – Общия регламент относно защитата на данните;

7. право на оттегляне на съгласието по всяко време, когато обработването на личните данни се основава на съгласие на лицето;

8. правото на жалба до надзорен орган – за Република България Комисията за защита на личните данни;

9. източника на данните;

10. съществуване на автоматизирано вземане на решения, включително профилиране;

11. данните, които идентифицират обработващия личните данни.

(2) Алинея 2 не се прилага, когато:

1. обработването е за статистически, исторически или научни цели и предоставянето на данните по ал. 1 е невъзможно или изисква прекомерни усилия;

2. вписването или разкриването на данни са изрично предвидени в закон;

3. физическото лице, за което се отнасят данните, вече разполага с информацията по ал. 1;

4. е налице изрична забрана за това в закон.

*Поддържани регистри на лични данни*

**Чл. 6.** В **ЧАСТНА ДЕТСКА ГРАДИНА”ВЪЛШЕБСТВО”** в качеството на дружеството на обработващ личните данни, е възложено да се обработват лични данни в следните регистри на други администратори на лични данни:

1. Регистър „Персонал“
2. Регистър „Клиенти”

**ІІІ. Регистър „Персонал“ на други администратори на лични данни, възложили на ЧАСТНА ДЕТСКА ГРАДИНА”ВЪЛШЕБСТВО”** **да обработва данните в него.**

*Общо описание на регистъра*

**Чл. 7.** В регистъра се обработват лични данни на кандидатите за работа при администраторите на лични данни, възложили на **ЧАСТНА ДЕТСКА ГРАДИНА”ВЪЛШЕБСТВО”** да ги обработва, и на служителите, работниците и изпълнителите по граждански договори с оглед:

1. индивидуализиране на трудови, служебни и граждански правоотношения;

2. изпълнение на нормативните изисквания на Кодекса на труда, Кодекса за социално осигуряване, Закона за счетоводството, Закона за данъците върху доходите на физическите лица, Закона за Националния архивен фонд и др.;

3. използване на събраните данни за съответните лица за служебни цели:

а) за всички дейности, свързани със съществуване, изменение и прекратяване на трудовите и граждански правоотношения;

б) за изготвяне на всякакви документи на лицата в тази връзка (договори, допълнителни споразумения, документи, удостоверяващи трудов стаж, служебни бележки, справки, удостоверения и др. подобни);

в) за установяване на връзка с лицето по телефон, за изпращане на кореспонденция, отнасяща се до изпълнение на задълженията му по трудови или граждански договори;

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

*Категории лични данни, обработвани в регистъра*

**Чл. 8.** В регистъра се обработват следните категории лични данни:

1. физическа идентичност: имена и паспортни данни (ЕГН, номер на лична карта, дата и място на издаване, адрес, месторождение, телефони за връзка и др.);

2. социална идентичност: данни относно образование и допълнителни квалификации (вид на образованието, място, номер и дата на издаване на дипломата), както и трудова дейност и професионална биография;

3. семейна идентичност: данни относно семейното положение на физическото лице (наличие на брак, развод, брой членове на семейството, в това число деца до 18 години);

4. икономическа идентичност: данни относно имотното и финансово състояние на физическото лице, участието и/или притежаването на дялове или ценни книжа на дружества и др.;

5. лични данни относно гражданскоправния статус на лицата, необходими за длъжностите, свързани с материална отговорност (напр. свидетелства за съдимост);

6. данни за здравословното състояние (медицинско свидетелство при постъпване на работа, периодични прегледи, преминавани с оглед характера на работата, изпълнявана по трудовото правоотношение и изискванията за безопасни условия на труд);

7. данни за членство в синдикални организации.

*Технологично описание на регистъра*

**Чл. 9.** (1) Технологичното описание на регистъра обхваща носителите на данни, технологията на обработване, срока за съхраняване и предоставяните услуги по регистъра.

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

(3) Данните в регистъра се предоставят от физическите лица при кандидатстване за работа при администраторите на лични данни, възложили на **ЧАСТНА ДЕТСКА ГРАДИНА”ВЪЛШЕБСТВО”** да ги обработва. Данните се въвеждат директно в договори, допълнителни споразумения, документи, удостоверяващи трудов стаж, служебни бележки, справки, удостоверения, кореспонденция и др.

(4) Данните в регистъра се съхраняват за срок от 50 години във връзка с нормативно установени срокове.

(5) Обработващият личните данни предоставя достъп, справки, извлечения, издаване на документи и други услуги от съответния регистър с лични данни.

*Длъжности, свързани с обработването и защитата на лични данни от регистъра и описание на техните права и задължения*

**Чл. 10.** (1) Данните от регистъра се обработват от Виолета Гинова Жекова, директор на обработващия данни **ЧАСТНА ДЕТСКА ГРАДИНА”ВЪЛШЕБСТВО”** , при спазване на принципа „Необходимост да се знае”.

(2) Длъжностните лица нямат право да разпространяват информация за личните данни, станали им известни при изпълнение на служебните им задължения.

*Оценка на въздействието на Регистър Персонал“*

**Чл. 11.** (1) Оценка на въздействието на Регистър „Персонал“ се извършва в съответствие с критериите по чл. 11, ал. 2 във връзка с чл. 14 от Наредба № 1 от 30 януари 2013 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни, при съобразяване със следните обстоятелства:

1. в регистъра се обработват лични данни за лица, чийто брой надхвърля 100, но не надхвърля 10 000;

2. в регистъра се обработват специални категории лични данни, свързани със здравословното състояние на работниците и служителите и данни за членство в синдикални организации с оглед прилагане на изискванията на трудовото законодателство.

(2) При отчитане на критериите по ал. 1, нивото на въздействие на Регистър „Персонал“ е средно.

(3) 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.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Оценка на нивото на въздействие на „Регистъра на служителите“ | | | | |
| **Наименование на**  **регистъра** | **НИВО НА ВЪЗДЕЙСТВИЕ** | | | |
| **поверителност** | **цялостност** | **наличност** | **общо за регистъра** |
| Персонал | средно | средно | средно | средно |

*Технически и организационни мерки за защита на личните данни в Регистър „Персонал“*

Съгласно условията на Регламент (ЕС) 2016/679 – Общия регламент относно защитата на данните: ”като се имат предвид достиженията на техническия прогрес, разходите за прилагане и естеството, обхватът, контекстът и целите на обработването, както и рисковете с различна вероятност и тежест за правата и свободите на физическите лица, администраторът и обработващият лични данни прилагат подходящи технически и организационни мерки за осигуряване на съобразено с този риск ниво на сигурност, включително, *inter alia/наред с другите неща/*, когато е целесъобразно:

a) псевдонимизация и криптиране на личните данни; 4.5.2016 г. L 119/51 Официален вестник на Европейския съюз BG

б) способност за гарантиране на постоянна поверителност, цялостност, наличност и устойчивост на системите и услугите за обработване;

в) способност за своевременно възстановяване на наличността и достъпа до личните данни в случай на физически или технически инцидент;

г) процес на редовно изпитване, преценяване и оценка на ефективността на техническите и организационните мерки с оглед да се гарантира сигурността на обработването.

….При оценката на подходящото ниво на сигурност се вземат предвид по-специално рисковете, които са свързани с обработването, по-специално от случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или достъп до прехвърлени, съхранявани или обработени по друг начин лични данни.”

В съзвучие с тази разпоредба на Регламента се разработват, утвърждават и внедряват мерките за физическа, документална, персонална защита и защита на информационните масиви от бази данни. Мерките се определят така, че да гарантират избягване на оценените рискове, да гарантират спазването на принципите при обработката на личните данни, но и да не създават допълнителни пречки при обработката на данните, които биха били затрудняващи фактори, но не биха допринесли за повишаване на сигурността на защитата на данните и не биха били допълнителна гаранция за спазване на принципите на обработка на личните данни. Администраторите на лични данни, възлагащи обработването им на **ЧАСТНА ДЕТСКА ГРАДИНА”ВЪЛШЕБСТВО”** се познават, одобряват и приемат предприетите мерки, надлежно разписани по- долу, и възлагайки обработката на личните данни от „Регистър Персонал”, се съгласяват, че същите са ефективни и адекватни.

**Чл. 12.** (1) Физическата защита на личните данни се осъществява при спазване на следните мерки:

1. Личните данни от регистъра се обработват в кабинетите на упълномощените по чл. 10 лица.

2. Всички документи на хартиен носител, съдържащи лични данни, се съхраняват в определени шкафове в кабинет, а достъпът до тях е ограничен само за упълномощени лица.

3. Елементите на комуникационно-информационните системи, използвани за обработване на лични данни се намират в шкаф, в помещение със зони, определени за тяхното съхранение.

4. Помещенията, в които се обработват лични данни от регистъра, са оборудвани със заключване на вратите и пожарогасителни средства.

5. Физическият достъп до зоните в обекта с ограничен достъп, включително и тези, в които са разположени елементи на комуникационно-информационните системи, е възможен само през заключващи се врати. Достъп се предоставя само на служителите, чийто служебни задължения включват обработване на лични данни от регистъра.

6. Външни лица имат достъп до помещенията, в които се обработват лични данни от регистъра, само в присъствието на упълномощени служители, но тези лица нямат достъп до шкафовете, в които се съхраняват личните данни. Целият директорски кабинет на **ЧАСТНА ДЕТСКА ГРАДИНА”ВЪЛШЕБСТВО”** , предвид естеството на основната дейност на обработващия личните данни- административна дейност, представлява помещение, което се достъпва единствено от лица, които са в трудово правни отношения с обработващия личните данни и са упълномощени да боравят с данните, съхранявани в него. Посещенията от външни лица се осъществява в приемна, отделена от зоните, в които се съхраняват документи, съдържащи лични данни под каквато и да било форма.

(2) Персоналната защита на личните данни се осъществява при спазване на следните мерки:

1. Лицата, обработващи лични данни, се запознават със ЗЗЛД, Наредба № 1 от 30 януари 2013 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни, настоящата Инструкция и правилата за информационна сигурност при постъпване на работа.

2. Лицата, обработващи лични данни, преминават обучение, включващо запознаване с политиката и ръководствата за защита на личните данни, запознаване с опасностите за личните данни, обработвани от администратора, като се провежда тренировка на персонала за реакция при събития, застрашаващи сигурността на данните.

3. Лицата, обработващи лични данни, са в трудово правни отношения с обработващият личните данни. Те задължително подписват декларация, с която поемат задължение за неразпространение на личните данни на работниците и служителите на администратора, възлагащ обработването, станали им известни във връзка и по време на изпълнение на служебните им задължения. Декларацията се съхранява в кадровото досие на всеки служител.

4. Споделяне на критична информация между служителите (като идентификатори, пароли за достъп и т.н.) е забранено от политиките за информационна сигурност.

(3) Документалната защита на обработваните в регистъра лични данни се осъществява при спазване на следните мерки:

1. Регистър „Персонал“ се поддържа на хартиен носител (кадрови досиета, чието съдържание съответства на нормативната уредба на Република България, както и на вътрешните нужди за периодична оценка на служителите), а отделни дейности по обработване на данните в него налагат поддържане на данни в електронен вид.

2. Обработването на личните данни се извършва в рамките на работното време на **ЧАСТНА ДЕТСКА ГРАДИНА”ВЪЛШЕБСТВО”**

3. Достъп до регистъра имат лицата по чл. 10 в съответствие с принципа „Необходимост да се знае”.

4. Личните данни се събират само с конкретна цел, в съответствие с нормативните изисквания към администратора. Данните се класифицират в съответствие с тяхното предназначение и характер и се съхраняват в шкаф в зоните с ограничен достъп.

5. Виолета Гинова Жекова е отговорна за контрол на достъпа до регистъра.

6. Сроковете за съхранение на документи от Регистър „Персонал“, които са на хартиен носител, са определени в чл. 9, ал. 4.

7. Документите се съхраняват в отредените за целта шкафове с ключ в **ЧАСТНА ДЕТСКА ГРАДИНА”ВЪЛШЕБСТВО”** .

8. Архивирането на документи се възлага на Виолета Гинова Жекова при спазване на съответните защитни мерки за определеното ниво на защита.

9. Личните данни могат да бъдат размножавани и разпространявани от упълномощените служители само ако е необходимо за изпълнение на служебни задължения или ако са изискани по надлежния ред от държавни органи или упълномощени лица.

10. Временните документи от регистъра, които са на хартиен носител и съдържат лични данни, се унищожават само чрез специално устройство (шредер).

11. След изтичане на срока за съхранение, или на друг период, не по- кратък от 1 година, или в случай, че администраторът на лични данни и обработващият личните данни прекратят договорните си взаимоотношения, документите от регистъра се предават на представител на администратора, възложил обработката на личните данни. Ако срокът за съхранение на личните данни не е изтекъл при предаването на документите от регистъра от обработващият личните данни на администратора, възложил обработването, последващото обработване/съхраняване/ се осъществява от администратора при съблюдаване на всички необходими правила и норми за това. Ако срокът за съхранение е изтекъл при предаването на документите от регистъра, същите се унищожават от администратора по надлежния ред- чрез физическото им унищожаване чрез изгаряне или по друг начин, определен от администратора.

(4) Защитата на автоматизирани информационни системи и мрежи се осъществява при спазване на следните мерки:

1. При работа с данните от регистъра се използват съответните софтуерни продукти за обработване. Данните се въвеждат в база данни и се съхраняват на сървър. Всеки упълномощен служител има личен профил (потребителско име и парола), с определени съобразно задълженията му права и нива на достъп. Дефинирани са и уникални потребителски имена и пароли за стартиране на операционната система на всеки един компютър.

2. Администраторът създава и поддържа стандартни и сигурни конфигурации за всяка компютърна и мрежова платформа, с която оперира, което включва стандартни и базови конфигурации за защита на операционната система, защитни стени, рутери и мрежови устройства. За защита на данните е инсталирана антивирусна програма и се извършва периодична профилактика на софтуера и системните файлове.

3.Директорът на обработващият личните данни Виолета Гинова Жекова е отговорен за управлението на регистъра. Само лицата посочени в чл. 10 имат достъп до регистъра.

4. За всички компютърни конфигурации, сървъри и комуникационни средства, от които зависи правилното поддържане на базите данни, са осигурени непрекъсваеми токозахранващи устройства (UPS).

5. В помещенията, в които са разположени компютърни и комуникационни средства, е осигурено заключване на помещенията, сигнално-охранителна система.

6.Допълнителни копия на носителите на информация, съдържащи лични данни, се съхраняват на сървър.

7. Контролът по използването на тези носители се осъществява от Виолета Гинова Жекова.

8. Организационни мерки за гарантиране нивото на сигурност:

а) Охрана на сградата с денонощна охрана, осъществявана от специализирано предприятие, извършващо охранителни услуги.

б) Забранено е използването на преносими лични носители на данни.

в) Работните компютърни конфигурации, както и цялата IT инфраструктура, включително и достъпът до интернет, се използват единствено за служебни цели.

г) При ремонт на компютърна техника, на която се съхраняват лични данни, предоставянето й на сервизната организация се извършва без устройствата, на които се съхраняват лични данни.

9. При предаване на документите от регистъра в електронен вид, извлечен от автоматизираната информационна система, съдържаща документите от регистъра от обработващия личните данни на администратора, възложил обработването им, се прилагат правилата на чл.12, ал.3, т.11 от настоящата инструкция. При желание от страна на администратора и след прекратяване на договорните отношения с обработващия личните данни, данните от регистъра биха могли да продължат да се съхраняват от обработващия личните данни. Преди прекратяване на взаимоотношенията с администратора и/или преди изтичане на срока за съхраняване на данните от регистъра, същите не се предават на администратора в електронен вариант, а се съхраняват по този начин само при обработващия личните данни.10. Сроковете за съхранение на данни от регистъра са описани в чл. 9, ал. 4.

(5) Криптографската защита при предаване на данни по електронен път или на преносими технически носители се осъществява чрез използване на стандартни технологии за криптиране на данните, както и използване на електронен подпис.

*Действия за защита при аварии, произшествия и бедствия*

**Чл. 13.** (1) При възникване и установяване на инцидент, веднага се докладва на лицето, отговорно за защитата на личните данни.

(2) За инцидентите се води дневник, в който задължително се вписват предполагаемото време или период на възникване, времето на установяване, времето на докладване и името на служителя, извършил доклада. След анализ на инцидента, упълномощено лице вписва в дневника последствията от инцидента и мерките, които са предприети за отстраняването им.

(3) В случаите на необходимост от възстановяване на данни, процедурата се изпълнява след писменото разрешение на Виолета Гинова Жекова , като това се отразява в дневника по архивиране и възстановяване на данни.

*Предоставяне на лични данни на трети лица*

**Чл. 14.** (1) Данни от регистъра могат да бъдат предоставяни на държавни институции с оглед изпълнение на нормативно задължение (НОИ, НАП, МВР и т.н.).

(2) В качеството си на обработващ личните данни, **ЧАСТНА ДЕТСКА ГРАДИНА”ВЪЛШЕБСТВО”** предоставя лични данни и на определени образователни институции (регионален инспекторат) във връзка с подаване на данни за децата записани в детската градина по договори с родителите. Личните данни, който се предоставят, са три имена и единен граждански номер и се предоставят с цел идентификация на лицето. Това се налага, с оглед изискванията на Министерството на образованието във връзка с образованието на деца. При наличие на изразено писмено желание от страна на лице, чиито данни се обработват от обработващия личните данни, други данни могат да бъдат предоставяне с оглед защитаване на интересите му пред трети страни.

*Срок за провеждане на периодични прегледи относно необходимостта от обработване/заличаване на данните*

**Чл. 15.** **ЧАСТНА ДЕТСКА ГРАДИНА”ВЪЛШЕБСТВО”** трябва да извършва ежегодни проверки на личните данни от регистъра на администратора, възложил обработката на данните, с оглед преценка на необходимостта от тяхното обработване и съответно ако е отпаднало задължението – за заличаването им.

*Ред за изпълнение на задълженията по чл. 25 от ЗЗЛД*

**Чл. 16.** (1)След изтичане на срока за съхранение на данните, комисия определя кои документи подлежат на унищожение и мястото на извършване на процедурата.

(2) Унищожението се извършва посредством няколко начина, определени в зависимост от наличните към момента на унищожението технически възможности за **ЧАСТНА ДЕТСКА ГРАДИНА”ВЪЛШЕБСТВО”** , а именно: чрез разрязване с помощта на машина – шредер и/или чрез изгаряне или разрушаване (отваряне) на корпуса на носителя на данни.

(3) В случай на прехвърляне на данните на друг администратор е необходимо да се уведоми КЗЛД, ако прехвърлянето е предвидено в закон и е налице идентичност на целите на обработването и се съставят съответно приемо-предавателни протоколи.

*Движение на личните данни между администратора на личните данни и обработващия данните, правила, които обработващият данните следва да спазва в съответствие с Регламент (ЕС) 2016/679 – Общия регламент относно защитата на данните, съхраняване и унищожаване на данните.*

Чл.17. (1)Движението на личните данни от администратора на личните данни до обработващия данните, на който това обработване е възложено от администратора, се предоставят или директно от физическите лица, за които се отнасят на обработващия данните, или на администратора на лични данни, който ги предава по подходящ начин на обработващия данните. Когато данните се предоставят на хартиен носител лично в офиса на обработващия личните данни, същите се предават от представител на администратора на личните данни, възложил на **ЧАСТНА ДЕТСКА ГРАДИНА”ВЪЛШЕБСТВО”** да обработва данните. Този представител е или управител на администратора, или лице, което е в трудови правоотношения с администратора и в длъжностната му характеристика е вменено задължението да обработва лични данни. При всички случаи администраторът следва да съхранява при себе си и да предостави и на обработващия данните декларация по чл.12, ал.2, т.3 от настоящата инструкция за всеки един от приносителите на личните данни на хартиен носител. По същия път обработващият личните данни може да придвижи документи, съдържащи лични данни от офиса на обработващия данните до офис/обект/ на администратора на личните данни- тези документи биха могли да бъдат предадени лично на управителя на администратора или на лице, което е в трудови правоотношения с администратора, ако тези лица имат подписани и предоставени декларации по чл.12, ал.2 , т.3 от настоящата инструкция.

Когато личните данни са представени за обработка по електронна поща, писмата следва да се изтриват в едномесечен срок от изпращането им.

Ако обработващият личните данни реши да използва при обработката им услугите на друг обработващ личните данни, задължително следва да получи разрешение за това от администратора, който му е възложил обработката.

**ІV. Регистър „Клиенти и/или доставчици“ на други администратори на лични данни, възложили на ЧАСТНА ДЕТСКА ГРАДИНА”ВЪЛШЕБСТВО”** **да обработва данните в него.**

*Общо описание на регистъра*

**Чл. 7.** В регистъра се обработват лични данни на клиентите и/или доставчиците/когато те са физически лица/ на администраторите на лични данни, възложили на **ЧАСТНА ДЕТСКА ГРАДИНА”ВЪЛШЕБСТВО”** да ги обработва, с оглед:

1. индивидуализиране на търговски взаимоотношения;

2. изпълнение на нормативните изисквания на Закон за корпоративното подоходно облагане, Закон за Данък върху добавената стойност, Закона за счетоводството, Закона за данъците върху доходите на физическите лица, Закона за Националния архивен фонд и др.;

3. използване на събраните данни за съответните лица за служебни цели:

а) за всички дейности, свързани с издаване на фактури и тяхното осчетоводяване;

б) за изготвяне на всякакви документи на лицата в тази връзка (договори, фактури, известия към фактури др. подобни);

в) за установяване на връзка с лицето по телефон, за изпращане на кореспонденция, отнасяща се до търговските взаимоотношения между администратора и лицето;

г) за водене на счетоводна отчетност, удържане на дължими данъци и други дейности относно възнагражденията на посочените по-горе лица по граждански договори.

*Категории лични данни, обработвани в регистъра*

**Чл. 8.** В регистъра се обработват следните категории лични данни:

1. физическа идентичност: имена и паспортни данни (ЕГН, адрес, телефони за връзка и др.);

2.*Технологично описание на регистъра*

**Чл. 9.** (1) Технологичното описание на регистъра обхваща носителите на данни, технологията на обработване, срока за съхраняване и предоставяните услуги по регистъра.

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

(3) Данните в регистъра се предоставят от физическите лица при установяване на търговски взаимоотношения с администраторите на лични данни, възложили на **ЧАСТНА ДЕТСКА ГРАДИНА”ВЪЛШЕБСТВО”** да ги обработва. Данните се въвеждат директно в договори, фактури, известия към фактури, служебни бележки, справки, кореспонденция и др.

(4) Данните в регистъра се съхраняват за срок от 10 години във връзка с нормативно установени срокове.

(5) Обработващият личните данни предоставя достъп, справки, извлечения, издаване на документи и други услуги от съответния регистър с лични данни.

*Длъжности, свързани с обработването и защитата на лични данни от регистъра и описание на техните права и задължения*

**Чл. 10.** (1) Данните от регистъра се обработват от лицата, които са в трудово правоотношение с обработващия данни **ЧАСТНА ДЕТСКА ГРАДИНА”ВЪЛШЕБСТВО”** , в чиято длъжностна характеристика е определено задължение за обработване на данните на служителите и при спазване на принципа „Необходимост да се знае”.

(2) Длъжностните лица нямат право да разпространяват информация за личните данни, станали им известни при изпълнение на служебните им задължения.

*Оценка на въздействието на Регистър „Клиенти/родители”*

**Чл. 11.** (1) Оценка на въздействието на Регистър „Клиенти/родители “ се извършва в съответствие с критериите по чл. 11, ал. 2 във връзка с чл. 14 от Наредба № 1 от 30 януари 2013 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни, при съобразяване със следните обстоятелства:

1. в регистъра се обработват лични данни за лица, чийто брой надхвърля 100, но не надхвърля 10 000;

(2) При отчитане на критериите по ал. 1, нивото на въздействие на Регистър „Клиенти/родители” е средно.

(3) 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.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Оценка на нивото на въздействие на „Регистъра на служителите“ | | | | |
| **Наименование на**  **регистъра** | **НИВО НА ВЪЗДЕЙСТВИЕ** | | | |
| **поверителност** | **цялостност** | **наличност** | **общо за регистъра** |
| Клиенти и/или Доставчици | средно | средно | средно | средно |

*Технически и организационни мерки за защита на личните данни в Регистър* „Клиенти/родители“

Съгласно условията на Регламент (ЕС) 2016/679 – Общия регламент относно защитата на данните: ”като се имат предвид достиженията на техническия прогрес, разходите за прилагане и естеството, обхватът, контекстът и целите на обработването, както и рисковете с различна вероятност и тежест за правата и свободите на физическите лица, администраторът и обработващият лични данни прилагат подходящи технически и организационни мерки за осигуряване на съобразено с този риск ниво на сигурност, включително, *inter alia/наред с другите неща/*, когато е целесъобразно:

a) псевдонимизация и криптиране на личните данни; 4.5.2016 г. L 119/51 Официален вестник на Европейския съюз BG

б) способност за гарантиране на постоянна поверителност, цялостност, наличност и устойчивост на системите и услугите за обработване;

в) способност за своевременно възстановяване на наличността и достъпа до личните данни в случай на физически или технически инцидент;

г) процес на редовно изпитване, преценяване и оценка на ефективността на техническите и организационните мерки с оглед да се гарантира сигурността на обработването.

….При оценката на подходящото ниво на сигурност се вземат предвид по-специално рисковете, които са свързани с обработването, по-специално от случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или достъп до прехвърлени, съхранявани или обработени по друг начин лични данни.”

В съзвучие с тази разпоредба на Регламента се разработват, утвърждават и внедряват мерките за физическа, документална, персонална защита и защита на информационните масиви от бази данни. Мерките се определят така, че да гарантират избягване на оценените рискове, да гарантират спазването на принципите при обработката на личните данни, но и да не създават допълнителни пречки при обработката на данните, които биха били затрудняващи фактори, но не биха допринесли за повишаване на сигурността на защитата на данните и не биха били допълнителна гаранция за спазване на принципите на обработка на личните данни. Администраторите на лични данни, възлагащи обработването им на **ЧАСТНА ДЕТСКА ГРАДИНА”ВЪЛШЕБСТВО”** се познават, одобряват и приемат предприетите мерки, надлежно разписани по- долу, и възлагайки обработката на личните данни от „Клиенти/родители“, се съгласяват, че същите са ефективни и адекватни.

**Чл. 12.** (1) Физическата защита на личните данни се осъществява при спазване на следните мерки:

1. Личните данни от регистъра се обработват в кабинетите на упълномощените по чл. 10 лица.

2. Всички документи на хартиен носител, съдържащи лични данни, се съхраняват в определени шкафове в кабинет, а достъпът до тях е ограничен само за упълномощени лица.

3. Елементите на комуникационно-информационните системи, използвани за обработване на лични данни се намират в шкаф, в помещение със зони, определени за тяхното съхранение.

4. Помещенията, в които се обработват лични данни от регистъра, са оборудвани със заключване на вратите и пожарогасителни средства.

5. Физическият достъп до зоните в обекта с ограничен достъп, включително и тези, в които са разположени елементи на комуникационно-информационните системи, е възможен само през заключващи се врати. Достъп се предоставя само на служителите, чийто служебни задължения включват обработване на лични данни от регистъра.

6. Външни лица имат достъп до помещенията, в които се обработват лични данни от регистъра, само в присъствието на упълномощени служители, но тези лица нямат достъп до шкафовете, в които се съхраняват личните данни. Целият директорски кабинет на **ЧАСТНА ДЕТСКА ГРАДИНА”ВЪЛШЕБСТВО”** , предвид естеството на основната дейност на обработващия личните данни- административни услуги, представлява помещение, което се достъпва единствено от лица, които са в трудово правни отношения с обработващия личните данни и са упълномощени да боравят с данните, съхранявани в него. Посещенията от външни лица се осъществява в приемна, отделена от зоните, в които се съхраняват документи, съдържащи лични данни под каквато и да било форма.

(2) Персоналната защита на личните данни се осъществява при спазване на следните мерки:

1. Лицата, обработващи лични данни, се запознават със ЗЗЛД, Наредба № 1 от 30 януари 2013 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни, настоящата Инструкция и правилата за информационна сигурност при постъпване на работа.

2. Лицата, обработващи лични данни, преминават обучение, включващо запознаване с политиката и ръководствата за защита на личните данни, запознаване с опасностите за личните данни, обработвани от администратора, като се провежда тренировка на персонала за реакция при събития, застрашаващи сигурността на данните.

3. Лицата, обработващи лични данни, са в трудово правни отношения с обработващият личните данни. Те задължително подписват декларация, с която поемат задължение за неразпространение на личните данни на работниците и служителите на администратора, възлагащ обработването, станали им известни във връзка и по време на изпълнение на служебните им задължения. Декларацията се съхранява в кадровото досие на всеки служител.

4. Споделяне на критична информация между служителите (като идентификатори, пароли за достъп и т.н.) е забранено от политиките за информационна сигурност.

(3) Документалната защита на обработваните в регистъра лични данни се осъществява при спазване на следните мерки:

1. Регистър „Клиенти/родители“ се поддържа на хартиен носител /фактури, договори/, а отделни дейности по обработване на данните в него налагат поддържане на данни в електронен вид.

2. Обработването на личните данни се извършва в рамките на работното време на **ЧАСТНА ДЕТСКА ГРАДИНА”ВЪЛШЕБСТВО”** .

3. Достъп до регистъра имат лицата по чл. 10 в съответствие с принципа „Необходимост да се знае”.

4. Личните данни се събират само с конкретна цел, в съответствие с нормативните изисквания към администратора. Данните се класифицират в съответствие с тяхното предназначение и характер и се съхраняват в шкаф в зоните с ограничен достъп.

5. Лицата, които са в трудови правоотношения с обработващия личните данни, са отговорни за контрол на достъпа до регистъра.

6. Сроковете за съхранение на документи от Регистър „Клиенти/родители“, които са на хартиен носител, са определени в чл. 9, ал. 4.

7. Документите се съхраняват в отредените за целта служебни помещения в **ЧАСТНА ДЕТСКА ГРАДИНА”ВЪЛШЕБСТВО”**

8. Архивирането на документи се възлага на Виолета Гинова Жекова при спазване на съответните защитни мерки за определеното ниво на защита.

9. Личните данни могат да бъдат размножавани и разпространявани от упълномощените служители само ако е необходимо за изпълнение на служебни задължения или ако са изискани по надлежния ред от държавни органи или упълномощени лица.

10. Временните документи от регистъра, които са на хартиен носител и съдържат лични данни, се унищожават само чрез специално устройство (шредер).

11. След изтичане на срока за съхранение, или на друг период, не по- кратък от 1 година, или в случай, че администраторът на лични данни и обработващият личните данни прекратят договорните си взаимоотношения, документите от регистъра се предават на представител на администратора, възложил обработката на личните данни. Ако срокът за съхранение на личните данни не е изтекъл при предаването на документите от регистъра от обработващият личните данни на администратора, възложил обработването, последващото обработване/съхраняване/ се осъществява от администратора при съблюдаване на всички необходими правила и норми за това. Ако срокът за съхранение е изтекъл при предаването на документите от регистъра, същите се унищожават от администратора по надлежния ред- чрез физическото им унищожаване чрез изгаряне или по друг начин, определен от администратора.

(4) Защитата на автоматизирани информационни системи и мрежи се осъществява при спазване на следните мерки:

1. При работа с данните от регистъра се използват съответните софтуерни продукти за обработване. Данните се въвеждат в база данни и се съхраняват на сървър. Всеки упълномощен служител има личен профил (потребителско име и парола), с определени съобразно задълженията му права и нива на достъп. Дефинирани са и уникални потребителски имена и пароли за стартиране на операционната система на всеки един компютър.

2. Администраторът създава и поддържа стандартни и сигурни конфигурации за всяка компютърна и мрежова платформа, с която оперира, което включва стандартни и базови конфигурации за защита на операционната система, защитни стени, рутери и мрежови устройства. За защита на данните е инсталирана антивирусна програма и се извършва периодична профилактика на софтуера и системните файлове.

3.Директорът на обработващият личните данни Виолета Гинова Жекова е отговорен за управлението на регистъра. Само лицата посочени в чл. 10 имат достъп до регистъра.

4. За всички компютърни конфигурации, сървъри и комуникационни средства, от които зависи правилното поддържане на базите данни, са осигурени непрекъсваеми токозахранващи устройства (UPS).

5. В помещенията, в които са разположени компютърни и комуникационни средства, е осигурено заключване на помещенията, сигнално-охранителна система.

6.Допълнителни копия на носителите на информация, съдържащи лични данни, се съхраняват на сървър.

7. Контролът по използването на тези носители се осъществява от Виолета Гинова Жекова.

8. Организационни мерки за гарантиране нивото на сигурност:

а) Охрана на сградата с денонощна охрана, осъществявана от специализирано предприятие, извършващо охранителни услуги.

б) Забранено е използването на преносими лични носители на данни.

в) Работните компютърни конфигурации, както и цялата IT инфраструктура, включително и достъпът до интернет, се използват единствено за служебни цели.

г) При ремонт на компютърна техника, на която се съхраняват лични данни, предоставянето й на сервизната организация се извършва без устройствата, на които се съхраняват лични данни.

9. При предаване на документите от регистъра в електронен вид, извлечен от автоматизираната информационна система, съдържаща документите от регистъра от обработващия личните данни на администратора, възложил обработването им, се прилагат правилата на чл.12, ал.3, т.11 от настоящата инструкция. При желание от страна на администратора и след прекратяване на договорните отношения с обработващия личните данни, данните от регистъра биха могли да продължат да се съхраняват от обработващия личните данни. Преди прекратяване на взаимоотношенията с администратора и/или преди изтичане на срока за съхраняване на данните от регистъра, същите не се предават на администратора в електронен вариант, а се съхраняват по този начин само при обработващия личните данни.10. Сроковете за съхранение на данни от регистъра са описани в чл. 9, ал. 4.

(5) Криптографската защита при предаване на данни по електронен път или на преносими технически носители се осъществява чрез използване на стандартни технологии за криптиране на данните, както и използване на електронен подпис.

*Действия за защита при аварии, произшествия и бедствия*

**Чл. 13.** (1) При възникване и установяване на инцидент, веднага се докладва на лицето, отговорно за защитата на личните данни.

(2) За инцидентите се води дневник, в който задължително се вписват предполагаемото време или период на възникване, времето на установяване, времето на докладване и името на служителя, извършил доклада. След анализ на инцидента, упълномощено лице вписва в дневника последствията от инцидента и мерките, които са предприети за отстраняването им.

(3) В случаите на необходимост от възстановяване на данни, процедурата се изпълнява след писменото разрешение на Виолета Гинова Жекова , като това се отразява в дневника по архивиране и възстановяване на данни.

*Предоставяне на лични данни на трети лица*

**Чл. 14.** (1) Данни от регистъра могат да бъдат предоставяни на държавни институции с оглед изпълнение на нормативно задължение (НОИ, НАП, МВР и т.н.).

(2) В качеството си на обработващ личните данни, **ЧАСТНА ДЕТСКА ГРАДИНА”ВЪЛШЕБСТВО”** предоставя лични данни и на определени регионални образователни институциивъв връзка с подаване на данни на деца подлежащи на обучение и образование. Личните данни, който се предоставят, са три имена и единен граждански номер и се предоставят с цел идентификация на лицето, в чиято полза се извършва плащането. Това се налага, с оглед изискванията на образователните институции.. При наличие на изразено писмено желание от страна на лице, чиито данни се обработват от обработващия личните данни, други данни могат да бъдат предоставяне с оглед защитаване на интересите му пред трети страни.

*Срок за провеждане на периодични прегледи относно необходимостта от обработване/заличаване на данните*

**Чл. 15.** **ЧАСТНА ДЕТСКА ГРАДИНА”ВЪЛШЕБСТВО”** трябва да извършва ежегодни проверки на личните данни от регистъра на администратора, възложил обработката на данните, с оглед преценка на необходимостта от тяхното обработване и съответно ако е отпаднало задължението – за заличаването им.

*Ред за изпълнение на задълженията по чл. 25 от ЗЗЛД*

**Чл. 16.** (1)След изтичане на срока за съхранение на данните, комисия определя кои документи подлежат на унищожение и мястото на извършване на процедурата.

(2) Унищожението се извършва посредством няколко начина, определени в зависимост от наличните към момента на унищожението технически възможности за **ЧАСТНА ДЕТСКА ГРАДИНА”ВЪЛШЕБСТВО”** , а именно: чрез разрязване с помощта на машина – шредер и/или чрез изгаряне или разрушаване (отваряне) на корпуса на носителя на данни.

(3) В случай на прехвърляне на данните на друг администратор е необходимо да се уведоми КЗЛД, ако прехвърлянето е предвидено в закон и е налице идентичност на целите на обработването и се съставят съответно приемо-предавателни протоколи.

*Движение на личните данни между администратора на личните данни и обработващия данните, правила, които обработващият данните следва да спазва в съответствие с Регламент (ЕС) 2016/679 – Общия регламент относно защитата на данните; съхраняване и унищожаване на данните.*

Чл.17. (1)Движението на личните данни от администратора на личните данни до обработващия данните, на който това обработване е възложено от администратора, се предоставят или директно от физическите лица, за които се отнасят на обработващия данните, или на администратора на лични данни, който ги предава по подходящ начин на обработващия данните. Когато данните се предоставят на хартиен носител лично в офиса на обработващия личните данни, същите се предават от представител на администратора на личните данни, възложил на **ЧАСТНА ДЕТСКА ГРАДИНА”ВЪЛШЕБСТВО”** да обработва данните. Този представител е или управител на администратора, или лице, което е в трудови правоотношения с администратора и в длъжностна му характеристика е вменено задължението да обработва лични данни. При всички случаи администраторът следва да съхранява при себе си и да предостави и на обработващия данните декларация по чл.12, ал.2, т.3 от настоящата инструкция за всеки един от приносителите на личните данни на хартиен носител. По същия път обработващият личните данни може да придвижи документи, съдържащи лични данни от офиса на обработващия данните до офис/обект/ на администратора на личните данни- тези документи биха могли да бъдат предадени лично на управителя на администратора или на лице, което е в трудови правоотношения с администратора, ако тези лица имат подписани и предоставени декларации по чл.12, ал.2 , т.3 от настоящата инструкция.

Когато личните данни са представени за обработка по електронна поща, писмата следва да се изтриват в едномесечен срок от изпращането им.

Ако обработващият личните данни реши да използва при обработката им услугите на друг обработващ личните данни, задължително следва да получи разрешение за това от администратора, който му е възложил обработката.

**ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ**

Параграф първи. Инструкцията се приема на основание чл. 23, ал. 4 от Закона за защита на личните данни, чл. 19, т. 2 от Наредба № 1 от 30 януари 2013 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни и при спазване на сроковете по § 2 от Преходните и заключителни разпоредби на Наредба № 1 от 30 януари 2013 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни.

Параграф втори. Инструкцията, в частта си, отнасяща се до обработването на лични данни от **ЧАСТНА ДЕТСКА ГРАДИНА”ВЪЛШЕБСТВО”** в качеството си на обработващ личните данни след изрично възлагане на тази обработка от други администратори на лични данни се подчинява на принципите на чл. 28, ал.3 от Регламент (ЕС) 2016/679 – Общия регламент относно защитата на данните, а именно:

a) обработва личните данни само по документирано нареждане на администратора, включително що се отнася до предаването на лични данни на трета държава или международна организация, освен когато е длъжен да направи това по силата на правото на Съюза или правото на държава членка, което се прилага спрямо обработващия лични данни, като в този случай обработващият лични данни информира администратора за това правно изискване преди обработването, освен ако това право забранява такова информиране на важни основания от публичен интерес;

б) гарантира, че лицата, оправомощени да обработват личните данни, са поели ангажимент за поверителност или са задължени по закон да спазват поверителност;

в) взема всички необходими мерки съгласно член 32;

г) спазва условията по параграфи 2 и 4 за включване на друг обработващ лични данни;

д) като взема предвид естеството на обработването, подпомага администратора, доколкото е възможно, чрез подходящи технически и организационни мерки при изпълнението на задължението на администратора да отговори на искания за упражняване на предвидените в глава III права на субектите на данни;

е) подпомага администратора да гарантира изпълнението на задълженията съгласно членове 32—36, като отчита естеството на обработване и информацията, до която е осигурен достъп на обработващия лични данни;

ж) по избор на администратора заличава или връща на администратора всички лични данни след приключване на услугите по обработване и заличава съществуващите копия, освен ако правото на Съюза или правото на държава членка не изисква тяхното съхранение;

з) осигурява достъп на администратора до цялата информация, необходима за доказване на изпълнението на задълженията, определени в настоящия член, и позволява и допринася за извършването на одити, включително проверки, от страна на администратора или друг одитор, оправомощен от администратора. 4.5.2016 г. L 119/49 Официален вестник на Европейския съюз BG Предвид буква з) от първа алинея обработващият лични данни незабавно уведомява администратора, ако според него дадено нареждане нарушава настоящия регламент или други разпоредби на Съюза или на държавите членки относно защитата на данни.

.Когато обработващият лични данни включва друг обработващ лични данни за извършването на специфични дейности по обработване от името на администратора, чрез договор или друг правен акт съгласно правото на Съюза или правото на държава членка на това друго лице се налагат същите задължения за защита на данните, както задълженията, предвидени в договора или друг правен акт между администратора и обработващия лични данни, както е посочено в параграф 3, по- специално да предостави достатъчно гаранции за прилагане на подходящи технически и организационни мерки, така че обработването да отговаря на изискванията на настоящия регламент. Когато другият обработващ лични данни не изпълни задължението си за защита на данните, първоначалният обработващ данните продължава да носи пълна отговорност пред администратора за изпълнението на задълженията на този друг обработващ лични данни.

Към индивидуалните договори, сключени между **ЧАСТНА ДЕТСКА ГРАДИНА”ВЪЛШЕБСТВО”** и администратора на лични данни, възложил обработването на данните, се прилага извлечение от т. Б. и от Параграф втори на настоящата инструкция, която представлява неразделна част от тези договори и определя рамката, която се прилага от обработващия личните данни в сътрудничество с администратора на лични данни- възложител.