



УТВЪРЖДАВАМ:
ДИРЕКТОР
/Ж.ХИНТОЛАРСКА /

ИНСТРУКЦИЯ

ЗА ТЕХНИЧЕСКИ И ОРГАНИЗАЦИОННИ МЕРКИ И СРЕДСТВА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ, ОБРАБОТВАНИ ОТ ДЕТСКА ГРАДИНА 43 „ПИНОКИО“,

1. ОБЩИ ПОЛОЖЕНИЯ

- 1.1. Настоящата инструкция се издава на основание чл. 23, ал. 4 и чл. 24, ал. 4 от Закона за защита на личните данни (ЗЗЛД) и Регламент (ЕС) 2016/679
- 1.2. Настоящата инструкция регламентира обработването, поддържането и защитата на регистрите с лични данни, поддържани от Детската градина .

(1) Обработването на лични данни е всяко действие или съвкупност от действия, които могат да се извършват по отношение на личните данни с автоматични или други средства, като събиране, записване, организиране, съхранение, адаптиране или изменение, възстановяване, консултиране, употреба, разкриване или предаване, разпространяване, актуализиране или комбиниране, блокиране, заличаване или унищожаване на данните.

(2) Обработването на лични данни се състои и в осигуряване на достъп до определена информация само за лица, чиито служебни задължения или конкретно възложени задачи налагат такъв достъп.

1.3. ДГ 43 „Пинокио“ е администратор на лични данни по смисъла на чл. 3, ал. 1 от Закона за защита на личните данни (ЗЗЛД), чиито цели и средства за обработване на личните данни са определени със закон.

1.4. „Лични данни“ са всяка информация, отнасяща се до физическо лице, което е идентифицирано или може да бъде идентифицирано пряко или непряко чрез идентификационен номер или чрез един или повече специфични признания, свързани с неговата физическа, физиологична, генетична, психическа, психологическа, икономическа, културна или социална идентичност.

1.5 Инструкцията е задължителна за всички обработващи лични данни.

2. ПОДДЪРЖАНИ РЕГИСТРИ

- 2.1. Училишното поддържа следните регистри с лични данни:
 - 2.1.1. Регистър „Персонал“
 - 2.1.2. Регистър „Дена“

- 2.1.3. Регистър „Родители“
- 2.1.4. Регистър „Контрагенти“
- 2.1.5. Регистър „Лични лекари“
- 2.1.6. Регистър „Видеонаబлюдение“

ОБЩО ОПИСАНИЕ НА ПОДДЪРЖКАНИТЕ РЕГИСТРИ

3. РЕГИСТЪР „ПЕРСОНАЛ“

В Регистър „Персонал“ се обработват лични данни, свързани с педагогически и непедагогически персонал на ДГ 43 „Пинокио“. В това си качество на Администратор на лични данни, детската градина е необходимо да обработва описаните по-долу категории с лични данни на учителите и служителите, работещи в него с цел изпълнение на нормативните изисквания на Кодекса на труда и подзаконовите нормативни актове за прилагането му, Кодекса за социално осигуряване, Закона за счетоводството, Закона за Предучилищно и Училищно образование, и други,

3.1. Категории лични данни и цели на обработването

3.1.1. Данни за физическа идентичност

Имена, ЕГН, месторождение; адрес; телефон за връзка, имейл; паспортни данни/ лична карта(без да се прави ксерокопие); трудова книжка – при потвърдено писмено съгласие Личните данните са необходими за идентификация на лицето и за осигурителни, данъчни административни цели и служебни цели за обезпечаване на образователния процес.

3.1.2. Данни за икономическа идентичност

Данни за банковите сметки на учителите и служителите. Данните са необходими за изплащане на възнагражденията по трудови и граждански договори.

3.1.3. Данни за социална идентичност

Националност на физическото лице. Тези лични данни се събират с цел да се провери законовото право на лицето да работи;

Образованитето на физическото лице (вид на образованнието, място, номер и дата на издаване на дипломата). Данните са необходими с оглед спазване нормативни или установени със щатного разписние на длъжностите изисквания за заемане, респ. за освобождаване на длъжности от лицата, както и за други свързани с управлението на човешките ресурси цели, като участие на служителите в програми за допълнително обучение/квалификация и професионално развитие;

Трудова дейност - професионална биография. Данните са от значение при избора на подходящо за съответната длъжност лице, както и за други свързани с управлението на човешките ресурси цели, като участие на служителите в програми за допълнително обучение/квалификация и професионално развитие.

3.1.4. Семейна идентичност

Семейното положение на физическото лице (наличие на брак, развод, брой членове на семейството, в това число деца до 18 години). Данните са необходими при установяване правата на лицата за получаване на семейни добавки за деца до 18 години.

3.1.5. Чувствителни лични данни

Медицинско свидетелство за започване на работа. Данните са от значение при заемане на длъжности и изпълнение на функции по трудови правоотношения, изискващи висока степен на отговорност, пряка ангажираност и непосредствен досег с хора, както и при необходимост на съобразяване на условията на труд със специфичното здравословно състояние на лицето и в случаите, в които това се изисква от действащото законодателство.

Болнични листове и други медицински документи на служителя/работника, свързани с временна нетрудоспособност.

3.1.6. Други данни

Гражданско-правен статус на лицата, необходими за длъжностите, свързани с материала отговорност, напр. свидетелство за съдимост.

3.2. Основания за обработване

Личните данни се предоставят на Администратора на лични данни(АЛД) или от съответните лица, за които те се отнасят или от Директора на ДГ във всички случаи, когато е необходимо и след получуване на изрично и информирано съгласие (*Приложение № 1*) от лицето, за което се отнасят личните данни. Законовите основания за обработване на данните са посочени в Кодекса на труда, Закона за счетоводството, Закон за облагане на доходите на физическите лица, Кодекс за социално осигуряване и др. и имат за цел: да се включват в управлението на човешките ресурси и администрация, да се улеснят администриративните функции и оперирането на информационните технологии, за администриране на съществуващи и бъдещи бизнес договорености, и за продажби и маркетинг на продукти и услуги, както и да се осигури съответствие със законовите изисквания, права и задължения, включително данък върху доходите и задължителните осигуровки, за поддръжане и докладване на доклади, извършване на одити, съобразяване с изискванията на различните власти, ако е необходимо да се отговоря в случай на съдебен процес като призовки, търсене на законни права и средства за защита, защита при спорове и управление на каквито и да било вътрешни оплаквания или претенции и в съответствие с вътрешните политики и процедури.

3.3. Лица, на които данните могат да бъдат разкривани: физическите лица, за които се отнасят данните; на трети лица, по силата на договор; на лица, обработващи личните данни; на предвидени в закон държавни органи.

3.4. Технология на събиране и обработване

3.4.1. Личните данни в Регистър „Персонал“ се набирагат при постъпване/възлагане на работа по трудово или гражданско правоотношение на дадено лице, както и в процеса на кандидатстване и по време на интервю. Не се изискава и впоследствие прилага ксерокопие на документ за самоличност в личното трудово досие. В допълнение, някои лични данни се събират от други органи и публични регистри, в електронни и/или документи на хартиен носител, в качеството на работодател, чиито задачи включват разплащащателни/ осигурителни функции и функциите на човешките ресурси, както е описано по-горе.

3.4.2. В случаите, когато ДГ събира лични данни директно от служителите/работниците, съгласно чл. 13 от Регламент (ЕС) 2016/679 ,информира физическото лице за необходимостта от набиране на лични данни, категориите лични данни и целите, за които ще бъдат използвани личните данни, получателите или категориите получатели, на които личните данни могат да бъдат разкрити, задължителния или доброволен характер на предоставянето на личните данни и последствията от тяхното непредоставяне, както и правото на достъп до личните данни и правото на поправката им ако са неточни, срока за който ще се съхраняват личните данни (ако това е невъзможно критериите използване за определяне на този срок)

3.4.3. След одобрение на заявление за постъпване/възлагане на работа на лицето от директора, той следва да препрати на, счетоводителя, Завеждащ административно стопанска дейност/ЗАС/ заявление заедно с приложните към него документи, за оформяне възникването на валидно трудово или гражданско правоотношение, включително чрез изготвяне на трудов или граждansки договор на хартиен носител.

3.4.4. След подписването на трудовия/граждански договор, претпис се връчва на постъпващия.

Трудовия/граждансия договор заедно с останалите носители на лични данни се подрежда в кадрово досие, което се поставя в специален картотечен шкаф който се помещава в помещение, предназначено за самостоятелна работа на служителите от отдел „Администрация“, на които с тази правила е възложено да бъдат обработвани на лични данни.

3.4.5 Личното досие на лицето не се изнася извън сградата на администратора. Никое длъжностно или трето лице няма право на досиета на персонала на ДГ, освен ако същото е изисквано по надлежен път от органи на съдебната власт (съд, прокуратура, следствени органи). Достъпът на тези органи до личните данни на лицата е правомерен.

3.4.6. Личните данни на служителя се водят и съхраняват и на електронен носител. Компютъра на който се въвеждат данните е свързан в локална мрежа, но със защитен достъп до личните данни, който е непосредствен само от страна на обработващите на лични данни. При работа с данните се използват софтуерни продукти по обработка на данните, относно възнагражденията на персонала, в това число основни и допълнителни възнаграждения, данъчни и други (вноски по заеми, запори и пр.) задължения, трудов стаж, пристъпствени и неприступствени дни и други подобни. Софтуерните продукти са адаптирани към специфичните нужди на администратора на лични данни. Компютрите се помещават в изолирано помещение за самостоятелна работа на обработващите на лични данни отдел „Администрация“.

Достъп до операционната система, съдържаща файлове за обработка на лични данни, имат само обработващите на лични данни чрез парола за отваряне на тези файлове. Защитата на електронните данни от неправомерен достъп, повреждане, изгубване или унищожаване се осигурява посредством поддържане на антивирусни програми, периодично архивиране на данните на отделни дискове, както и чрез поддържане на информацията на хартиен носител.

3.4.7 При необходимост от Актуализация на личните данни предствляваща допълнение или изменение на съществуваща информация в ДГ . Актуализация на лични данни се извършва:

- по искане на лицето(**Приложение 2**), за което се отнасят личните данни, когато то е установило, че е налице грешка или непълнота в тях, и удостовери това с документ;
- по инициатива на обработващия лични данни – при наличие на документ, даващ основание за актуализация;
- при установена грешка при обработката на личните данни от страна на

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

3.4.8. При гореописаните случаи, силно ограничен достъп до лични данни има само от Счетоводителя и касиера във връзка с изготвяне на разплащателни документи, за преводи на възнагражденията на лицата, наети по трудови и граждански правоотношения по банков път, както и във връзка със заплащането на данъчни и осигурителни задължения, подаване на декларации и други данни в тази връзка към компетентните органи и изпълнението на други нормативно определени задължения на работодателя.

3.4.9. Личните данни от Регистър „Персонал“ се съхраняват на хартиен, технически и/или електронен носител в предвидените в нормативен акт срокове. След изтичане на установения срок те се осъществяване на законовите задължения на ДГ само от директора. Унищожават по заповед на директора на ДГ , като за изпълнението се съставя надлежен протокол. Личните данни могат да бъдат заличени и по желание на лицето след предоставено искане (Приложение 3)

3.4.10. Пренос на личните данните от Регистър „Персонал“ по електронен път се извършва при осъществяване на необходимото ниво на защита в съответствие с действащото законодателство с цел осъществяване на законовите задължения на ДГ само от директора.

3.4.11. ДГ може да предоставя личните данни от Регистър „Персонал“ на трети лица- обработващи личните данни от името на Директора в съответствие с определените в тази Инструкция цели и ред и при осигуряване на необходимата защита. Решението си за предоставяне или отказване

достъп до лични данни за съответното лице администраторът съобщава на третите лица в 30-дневен срок от подаване на молбата, resp. искането.

3.4.12. Не се изисква съгласие на лицето, ако обработването на неговите лични данни се извършва само от или под контрола на компетентен държавен орган за лични данни, свързани с извършване на престъпления, на административни нарушения и на непозволени увреждания. На такива лица се осигурява достъп до личните данни, като при необходимост им се осигуряват съответни условия за работа в помещение на ДГ

3.4.13. Правомерен е и достъпът на ревизиращите държавни органи, надлежно легитимирали се със съответни документи – писмени разпореждания на съответния орган, в които се посочва основанието, имената на лицата, като за целите на дейността им е необходимо да им се осигури достъп до личните досигета на персонала.

3.4.14. Защитата на личните данни в Регистър „Персонал“ се осигурява чрез предвидените мерки в тази Инструкция.

4. РЕГИСТЪР „ДЕЦА“

В Регистър „ДЕЦА“ се обработват лични данни, свързани с дейността на ДГ 43“Пинокио“

4.1. Категории лични данни и цели на обработването

В Регистър „ДЕЦА“ се обработват:

4.1.1. Данни за физическа идентичност- имена ЕГН; адрес; телефон за връзка; дата на раждане. Данните са необходими за идентификация на лицето, както и за изпълнение на задължения, записани в ЗПУО и нормативните документи от системата на МОН , участие в конференции и проекти в РБ от Европейския съюз , за всички дейности, свързани с изготвяне на всякаакви документи и справки за лицата (служебни бележки, справки, уверение, удостоверения и др. подобни

4.1.2 Медицински данни – Медицинска здравно-профилактична карта, Копие на Имунизационен картон, ТЕЛК

4.1.3.Други данни – личен лекар.

4.2. Основания за обработване

Личните данни се предоставят на АДЛ от техните законни представители на основание нормативно задължение – ЗПУО, всички наредби определящи ДОС, Закона за закрила на детата, когато е необходимо, след получаване на изрично и информирано съгласие (**Приложение 4**)

4.3. Лица, на които данните могат да бъдат разкривани: на физическите лица, за които се отнасят данните, респективно на техните родители/настойници; на трети лица по силата на договор или ЗПУО, на лица, обработващи личните данни; на предвидени по закон държавни органи, а на чуждестранни физически и/или юридически лица, извън територията на Република България и Европейския съюз само след разрешение на КЗЛД. За тези действия физическите лица, чрез техните законни представители, трябва предварително да бъдат уведомявани, преди да им се обработват личните данни.

4.4. Технология на събиране и обработване

4.4.1. Информация за Децата може да бъде събрана от ДГ , по телефон и/или интернет и имейл, чрез представителите на ръководството, директор, учители ,ЗАС

4.4.2. Личните данни в Регистър „ДЕЦА“ се събират от ДГ директно от родителите/настойниците,ДГ информира родителя /настийник за нуждата за тяхното събиране, категорията лични данни, които се събират, причината за тяхното обработване, получателите или

категориите получатели, на които данните могат да бъдат разкрити, задължителния или доброволен характер на съхраняването на данни и последиците ако същите не бъдат предоставени, както и правото на досъп и правото да се поправят данните, ако същите са неправилни, срока за който ще се съхраняват личните данни (ако това е невъзможно критериите използвани за определяне на този срок)

4.4.3. Когато има нужда от корекция или актуализация на личните данни , Родителя/Настойника на детето за което се отнасят данните, предоставя правилните и актуализирани данни директно или чрез свързване онлайн или по телефон.Актуализацията се извършва по желание на ДГ или по желание на Родителя /Настойника на детето чрез заявление (Приложение 2)

4.4.4. В горепосочените случаи, ограничен достъп до личните данни може да бъде предоставен на служителите, които се нуждаят от достъпа въз основа на принципа „*Необходимост да знае*“ , за предоставяне на данни на компетентни органи и изпълнение на други законови задължения на АДД.

4.4.5. Личните данни, които се съдържат в Регистър „ ДЕЦА ” ще се въвеждат на хартиен носител в папки за всяко дете . Досиетата се ще подреждат и съхраняват в шкафове. Шкафове ще се помещават по групите .На технически носител, личните данни се въвеждат на твърд диск, на изолиран компютър в стаята на „Администрацията“ . Компютърът е свързан в локална мрежа, но със защитен достъп до личните данни, който е непосредствен само от страна на обработващите на лични данни. При работа с данните се използва софтуерен продукт „ Такси „, по обработка на данните.Компютърите се поместват в помещения за работа на обработващите на данните по регистъра.

4.4. 6. Личните данни се съхраняват на хартиен и технически носител за времето основателно необходимо за целите, за които данните са били събрани или за кое то е далено съгласие от Родителя /Настойника на детето , или е необходимо за изпълнение на правните задължения на Директора. Данните ще бъдат унищожени при изтичане на съответния период по заповед на директора на ДГ , като за изпълнението се съставя надлежен протокол. Личните данни могат да бъдат заличени и по желание на Родителя /Настойник след предоставено искане (Приложение 3)

4.4.7. Електронният пренос на личните данни се осъществява при осигуряване на защита, програма за защита на системата от външни лица, актуализирана антивирусна и антидостъп защити, както и виртуална частна мрежа за дистанционен достъп, в съответствие с приложимото законодателство, за да може ДГ да изпълнява законните си задължения и за други нужди посочени в тази Инструкция, както и в съответствие със законодателството приложимо към защита на личните данни.

4.4.8. ДГ може да предоставя лични данни от Регистър „ДЕЦА “ на трети лица, действащи като обработващ лични данни от името на ДГ за нуждите описани в настоящото и при осигуряване на нивото на защита.

4.4.9. Защитата на личните данни в Регистър „ Деца “ се осигурява чрез мерките, предвидени в тази Инструкция.

5.РЕГИСТЪР „РОДИТЕЛИ“

5.1. Категории лични данни и цели на обработването

В Регистър „Родители“ се обработват лични данни, свързани с родителите/ настойниците на децата в детската градина . В Регистър „Родители“ се обработват:

5.1.1. Данни за физическа идентичност- имена; адрес; телефон за връзка;

Данните са необходими за идентификация на лицето, както и за изпълнение на задължения, записани в ЗПУО.

5.1.2 Медицински данни за родителите - документ за нетрудоспособност (в определени случаи)
Данните са необходими за във връзка с определение на преференции на таксите на детето

5.2. Основания за обработване

Личните данни от лицата се предоставят на АЛД на основание нормативно задължение - ЗПУО, всички наредби определящи ДОС, Закона за закрила на децата, когато е необходимо, след получаване на изрично и информирано съгласие от лицето (**Приложение 4**) , за което се отнасят личните данни.

5.3. Лица, на които данните могат да бъдат разкривани: на физическите лица, за които се отнасят данните; на трети лица по силата на договор или ЗПУО, ; на лица, обработващи личните данни; на предвидени по закон държавни органи, а на чуждестранни физически и/или юридически лица, извън територията на Република България и Европейския съюз само след разрешение на КЗЛД. За тези действия физическите лица трябва предварително да бъдат уведомявани, преди да им се обработват личните данни.

5.4. Технология на събиране и обработване

5.4.1. Информация за родителя може да бъде събрана пряко, онлайн от ДГ, като например, по телефон, чрез представителите на ръководството – учители , директор ,ЗАС и мед. Сестра .

5.4.2. Личните данни в Регистър „ Родители” се събират от ДГ директно от родителите/настайниците ,съгласно чл. 13 от Регламент (ЕС) 2016/679 ,ДГ ще информира лицето, за нуждата за тяхното събиране, категорията лични данни, които се събират, причината за тяхното обработване, получателите или категориите получатели, на които данните могат да бъдат разкрити, задължителния или доброволен характер на съхраняването на данни и последиците ако същите не бъдат предоставени, както и правото на достъп и правото да се поправят данните, ако същите са неправилни. Ако е приложимо, лицето за което се отнасят личните данни, ще бъде информиран, също и за останалите случаи по чл. 20 от Закона за защита на личните данни.

5.4.3. Когато има нужда от корекция или актуализация, лицето за което се отнасят данните, предоставя на директора или съответния служител правилните и актуализирани данни Актуализацията се извършва по желание на ДГ или по желание на лицето чрез заявление (**Приложение 2**)

5.4.4. В горепосочените случаи, ограничен достъп до личните данни може да бъде предоставен на служителите, които се нуждаят от достъпа, въз основа на принципа „Необходимост да знае“ за предоставяне на данни на компетентни органи и изпълнение на други законови задължения на АЛД.

5.4.5. Личните данни, които се съдържат в Регистър „ Родители” ще се съхраняват на хартиен, технически и/или електронен носител за времето основателно необходимо за целите, за които данните са били събрани или за което е дадено съгласие от лицето, или е необходимо за изпълнение на правните задължения на Директора.

5.4.6. Електронният пренос на личните данни(ако такъв се налага), се осъществява при осигуряване на защита, програма за защита на системата от външни лица, актуализирана антивирусна и анти-достъп за защити, както и виртуална частна мрежа за дистанционен достъп, в съответствие с приложимото законодателство, за да може ДГ да изпълнява законните си задължения и за други нужди посочени в тази Инструкция, както и в съответствие със законодателството приложимо към защита на личните данни.

5.4.7. ДГ може да предоставя лични данни от Регистър „ Родители” на трети лица, действащи като обработващ лични данни от името на ДГ за нуждите описани в настоящото и при осигуряване на нивото на защита.

5.4.8. Личните Данните ще бъдат унищожени при изтичане на съответния период по заповед на директора на ДГ , като за изпълнението се съставя надлежен протокол. Личните данни могат да бъдат заличени и по желание на лицето след предоставено искане (**Приложение 3**)

5.4.9. Защитата на личните данни в Регистър „Родители“ се осигурява чрез мерките, предвидени в тази Инструкция.

6. РЕГИСТЪР „КОНТРАГЕНТИ“

6.1. Категории лични данни и цели на обработването

В Регистър „Контрагенти“ се обработват само нечувствителни данни.

6.1.1. Данни за физическа идентичност - имена; адрес; телефон за връзка;

Данните са необходими за идентификация на лицето, за необходимата кореспонденция с доставчика и за счетоводни цели.

6.1.2. Данни за икономическа идентичност

Данните за кредитните карти и финансовото състояние на доставчичите. Данните са необходими за счетоводни цели.

6.2. Основания за обработване

Обикновено данните събиращи от доставчичите се отнасят до юридическо лице и могат да включват информация за съответното лице за контакт с това юридическо лице. В повечето случаи, търговският договор с доставчика е между ДГ и доставчика. ДГ получава данните на доставчика и като част от управлениките си задължения, ще обработва данните за цели, свързани с бизнес взаимоотношенията и за данъчни и разплащателни нужди.

6.3. Лица, на които данните могат да бъдат разкривани: физическите лица, за които се отнасят данните; на трети лица по силата на договор; на лица, обработващи личните данни; на предвидени по закон държавни органи, а на чуждестранни физически и/или юридически лица, извън територията на Република България и Европейския съюз само след разрешение на КЗЛД. За посочените действия физическите лица трябва предварително да бъдат информирани.

6.4. Технология на събиране и обработване

6.4.1. Личните данни в регистър „Контрагенти“ ще бъдат събрани със започване на бизнес отношенията по силата на договор между ДГ и Доставчика. Както е посочено по-горе, събранныте данни могат да съдържат информация, във връзка с доставчика и техният/те служител/и, които изпълняват ролята на лице за контакт, както и информация, която е необходима за администриране на взаимоотношенията с доставчика, включително и за извършване на плащания към него.

6.4.2. Личните данни, събиращи от доставчика включват ограничено количество информация, необходима за връзка и управление на взаимоотношенията с доставчика; тази информация се използва само за тези цели.

6.4.3. Личните данни, които са свързани с Доставчика ще бъдат съхранявани на защитен с парола електронен носител, достъпен за служители от Счетоводството, които са отговорни за управление на бизнес отношенията. Достъп на други служители ще бъде разрешаван само със специално разрешение дадено от директора на база принципа „Необходимост да знае“.

6.4.4. Когато има необходимост от корекция или актуализация, лицето трябва да предаде на служителя в Администрацията, който управлява бизнес взаимоотношението с доставчика коригираните или актуализирани данни.

6.4.5. В случаите по-горе, служителите от Администрацията ще получават достъп до личните данни въз основа на принципа „Необходимост да знае“, във връзка със следното: подготвяне на платежни документи необходими за извършване на банкови преводи за заплащане на възнаграждения; заплащане на данъчни задължения; и изпълнение на други задължения установени със закон.

6.4.6. Личните данни, които се съхраняват в Регистър „Контрагенти“ се съхраняват на хартиен, технически и/или електронен носител, само за времето, необходимо за управление на взаимоотношението с доставчика, колкото е необходимо за счетоводните нужди на Администратора на личните данни и/или за изпълнение на правни задължения на директора. Данните ще бъдат унищожени при изтичане на посочения период по заповед на директора на ДГ, като за изпълнението се съставя надлежен протокол

6.4.7. Данните на хартиен носител свързани с доставчите ще бъдат съхранявани по сигурен начин в Счетоводството, в съответствие с принципите, посочени по-долу.

6.4.8. Електронното пренасяне на лични данни(ако такъв се налага), ще се осъществява при осигуряване на адекватно ниво на защита в съответствие с приложимото законодателство, за да може Дружеството да изпълнява законовите си задължения.

6.4.9. ДГ може да предоставя лични данни от Регистър „Контрагенти“ на трети лица, действащи като обработващи лични данни от името на Дружеството за нуждите, описани в настоящата Инструкция, в предвидените в закон случаи и при осигуряване на адекватно ниво на защита.

6.5. Защитата на личните данни в Регистър „Контрагенти“ се осигурява чрез мерките и средства, предвидени в тази Инструкция.

7. РЕГИСТЪР „ЛИЧНИ ЛЕКАРИ“

7.1. Категории лични данни и цели на обработването

В Регистър „Лични лекари“ се обработват лични данни, свързани с лекарите педиатри, лекувачи деца от детската градина . В Регистър „Лични лекари“ се обработват само нечувствуителни данни.

7.1.1. Данни за физическа идентичност- имена; телефон за връзка;

Данните са необходими за идентификация на лицето, както и за изпълнение на задължения на медицинския специалист, записани в закон.

7.2. Основания за обработване

Личните данни от лицата се предоставят на АЛД на основание нормативно задължение - ЗПУО, Закона за закрила на децата, когато е необходимо,

7.3. Лица, на които данните могат да бъдат разкривани: на физическите лица, за които се отнасят данните; на трети лица по силата на договор; на лица, обработващи личните данни; на предвидени по закон държавни органи – Министерство на здравеопазването, а на чуждестранни физически и/или юридически лица, извън територията на Република България и Европейския съюз само след разрешение на КЗЛД. За тези действия физическите лица трябва предварително да бъдат уведомявани, преди да им се обработват личните данни.

7.4. Технология на събиране и обработване

7.4.1. Информация за личния лекар може да бъде събрана пряко онлайн от ДГ , като например, по телефон, чрез представителите на ръководството - учители и мед.сестри .

7.4.2. Личните данни в Регистър „Лични лекари“ се събират от ДГ директно от родителите/настойниците.

7.4.3. Когато има нужда от корекция или актуализация, лицето за което се отнасят данните, предоставя правилните и актуализирани данни на служителите чрез свързване онлайн или по телефон.

7.4.4. В горепосочените случаи, ограничен достъп до личните данни може да бъде предоставен на служителите, които се нуждаят от достъпа въз основа на принципа „Необходимост да знае“, за представяне на данни на компетентни органи и изпълнение на други законови задължения на Администратора на лични данни.

7.4.5. Личните данни, които се съдържат в Регистър „Лични лекари“ ще се съхраняват на хартиен, технически и/или електронен носител за времето основателно необходимо за целите, за които данните са били събрани, или за което е дадено съгласие от лицето, или е необходимо за изпълнение на правните задължения на Директора. Данните ще бъдат унищожени при изтичане на съответния период или отпадане на горното качество по заповед на директора на ДГ, като за изпълнението се съставя надлежен протокол.

7.4.6. Електронният пренос на личните данни(ако такъв се налага) се осъществява при осигуряване на защита, програма за защитата на системата от външни лица, актуализирана антивирусна и антидостъп защита, както и виртуална частна мрежа за дистанционен достъп, в съответствие с приложимото законодателство, за да може ДГ да изпълнява законните си задължения и за други нужди посочени в тази Инструкция, както и в съответствие със законодателството приложимо към защита на личните данни.

7.4.7. ДГ може да предоставя лични данни от Регистър „Лични лекари“ на трети лица, действащи като обработващ лични данни от името на ДГ за нуждите за опазване здравето на детето и при осигуряване на нивото на защита.

7.4.8. Защитата на личните данни в Регистър „Лични лекари“ се осигурява чрез мерките, предвидени в тази Инструкция.

8. РЕГИСТЪР „ВИДЕОНАБЛЮДЕНИЕ“

8.1. Общо описание на регистъра
8.2. Цели на обработване на лични данни: Охранителна дейност, осъществявана от ДГ „43“Пинокио“

8.3. Нормативно основание: ЗПУО,

8.4. Категории физически лица, на които се обработват данните: Деца , Родители на децата , служители, посетители.

8.5. Категории лични данни: Видеоматериал.

8.6. Източници, от които се събират данните:

- от зоните, в които се води видеонаблюдението, които са обозначени с информационни табели.

8.7. Технологично описание на регистъра

8.8. Носители на данни

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

8.9. Технология на обработване

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

8.10. Срок на съхранение

Данните в регистър „Видеонаблюдение“ се съхраняват 30 дни.

8.11. Предоставени услуги

ДГ „43“Пинокио“ не обработва личните данни от регистър „Видеонаблюдение“ за други цели, извън посочените в т. 9.2. от настоящата инструкция.

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

8.13. Данните от регистър „Видеонаблюдение“ се обработват при спазване на принципа „Необходимост да се знае“ от служителите, свързани с обработването на личните данни от регистър „Видеонаблюдение“.

8.14. Достъп до данните имат само, директора на ДГ, служителите свързани с обработването на личните данни от регистър „Видеонаблюдение“, и компетентните органи на МВР.

ТЕХНОЛОГИЧНО ОПИСАНИЕ НА ПОДДЪРЖКАНИТЕ РЕГИСТРИ

1. Носители на данни

Директорът може да съхранява категориите лични данни, съдържащи се в регистрите по т. 2, на хартиени или технически и/или електронни носители при спазване на приложимото законодателство и необходимите мерки за защита.

1.1. Срок на съхранение

Личните данни в Регистрите по чл. 2 се съхраняват за периода необходим за изпълнение на правните и бизнес нужди на ДГ, в зависимост от съответния регистър, категорията лични данни и целите за обработката им. Личните данни няма да се съхраняват по-дълго, отколкото е необходимо за защитата на законните интереси на ДГ 43 „Пинокио“ или за счетоводни цели, или в съответствие с изискванията на приложимите местни закони. Данните, обработвани ДГ 43 „Пинокио“ ще бъдат унищожени след изтичане на периода на пазене, в съответствие с изискванията, изложени в тази Инструкция.

1.1.1. Сроковете за съхранение по отделните регистри са както следва:

- Регистър „Персонал“ – 50 години
- Регистър „Деца“ – 5 години
- Регистър „Родители“ – 5 години
- Регистър „Контрагенти“ – 7 години
- Регистър „Лични лекари“ – 5 години
- Регистър „Видеонаблюдение“ – 30 дни

2. Дължностите, свързани с обработване и защита на лични данни, правата и задълженията им

2.1. Дължностите, свързани с обработване и защита на лични данни, правата и задълженията им, определени в тази точка са приложими за всички Регистри, изброени в настоящата Инструкция.

2.2. Должностното лице по защита на личните данни е директорът и отговаря за контрола върху достъпа и използването на личните данни.

2.3. Директорът има следните правомощия:

- 2.3.1. Осигурява организацията по водене на регистрите, съгласно предвидените мерки за гарантиране на адекватна защита;
- 2.3.2. Осъществява контрол по спазване на изискванията за защита на регистрите;
- 2.3.3. Поддържа връзка с Комисията за защита на личните данни относно предприетите мерки и средства за защита на регистрите и подадените заявления за предоставяне на лични данни.
- 2.3.4. Специфицира техническите ресурси, прилагани за обработка на личните данни;
- 2.3.5. Следи за спазване на организационните процедури за обработване на личните данни и за спазване на контролирания достъп до носителите на лични данни;
- 2.3.6. Провежда периодичен контрол за спазване на изискванията по защита на данните и при открити нередности взема мерки за тяхното отстраняване.

2.4. Достъп до личните данни, съхранявани в Регистрите имат само служителите на „ДГ“, на които такъв достъп е необходим за изпълнение на служебните им задължения, както и за изпълнение на бизнес цели, при стриктно спазване на принципа „Необходимост да знае“

2.4.1. По-конкретно тези служители са директор, ЗАС, учители, главен счетоводител Техн Изпитнител, мед.специалист, както и други лица, упълномощени на принципа „Необходимост да знае“. Възможността за достъп до личните данни при обработката им, на други служители в ДГ е ограничена до случаите, когато на тях изрично е предоставено такова право на достъп и в съответствие с принципа „Необходимост да знае“. Правото на достъп се предоставя за всеки конкретен случай на служителят, на когото се дава достъп, с изрично разрешение, в което се посочват личните данни и целите, за които се предоставя достъпът, както и времето, за което той се предоставя.

2.6. Тези служители, както и други лица, на които е възложено обработването на лични данни от Регистрите са длъжни: да обработват личните данни законоъобразно и добросъвестно; да използват личните данни, до които имат достъп, съобразно целите, за които се събират и да не ги обработват допълнително по начин, несъвместим с тези цели; да актуализират регистрите с личните данни (при необходимост); да различават или коригират личните данни, когато се установви, че са неточни или непропорционални по отношение на целите, за които се обработват; да поддържат личните данни във вид, който позволява идентифициране на съответните физически лица за период не по-дълъг от необходимия за целите, за които тези данни се обработват, да спазва тази Инструкция, както и другите корпоративни правила.

3. Мерки за защита при обработване на личните данни

3.1 Правилата за защита при обработване на лични данни регламентират технически мерки, които:

- 3.1.1** отхвърлят достъпа на неоторизирани лица до оборудването за обработка на данни – контрол на достъпа до оборудване;
- 3.1.2** предотвратяват неоторизираното четене, копиране, промяна или унищожаване на информационни носители – контрол на информационните носители;
- 3.1.3** предотвратяват неоторизираното добавяне, въвеждане, преглеждане, промяна или заличаване на съхранени лични данни – контрол по съхраняването;
- 3.1.4** предотвратяват използването му от неоторизирани лица, използваци комуникационно оборудване за данни – контрол на потребителите;
- 3.1.5** гарантират, че лицата, които са оторизирани да ползват система за автоматизирана обработка на данни, имат достъп само до данните, включени в обхвата на техния достъп – контрол на достъпа до данни;
- 3.1.6** осигуряват възможността за проверка и установяване до кои органи са били или могат да бъдат изпратени или предоставени личните данни чрез използване на комуникационно оборудуване за данни – контрол на комуникациите;
- 3.1.7** осигуряват възможност за последваща проверка и установяване какви лични данни са въведени в системите за автоматизирана обработка на данни, кога и от кого са въведени данните – контрол на въвеждане;
- 3.1.8** предотвратяват неоторизирано четене, копиране, промяна или изтриване на лични данни при трансфер на лични данни или превозване на носители на данни – контрол при транспортиране;
- 3.1.9** осигуряване на възможност инсталирани системи да могат да се възстановят в случаи на прекъсване на функционирането – възстановяване;
- 3.1.10** осигуряват правилното функциониране на системата, докладване на появата на грешки във функциите (надеждност) и гарантират, че съхранените данни не могат да бъдат повредени чрез неправилно функциониране на системата – интегритет.

4. Принципи за защита на личните данни

4.1 Принцип на ограничено събиране – събирането на лични данни трябва да бъде в рамките на необходимото. Информацията се събира по законен и обективен начин;

4.2 Принцип на ограничено използване, разкриване и съхранение – личните данни не трябва да се използват за цели, различни от тези, за които са били събиранни, освен със съгласието на лицето или в случаите, изритично предвидени в закона. Личните данни трябва да се съхраняват само толкова време, колкото е необходимо за изпълнението на тези цели;

4.3 Принцип на прецизност – личните данни трябва да са прецизни, точни, пълни и актуални, доколкото това е необходимо за целите, за които се използват;

4.4 Принцип на сигурността и опазването – личните данни трябва да са защитени с мерки за сигурност, съответстващи на чувствителността на информацията.

5. Мерки за защита на личните данни :

5.1. Всички хартиени и електронни записи, се съхраняват и са ограничени само за служители, които трябва да имат достъп чрез принципа „*Необходимост да знае*“, с оглед изпълнението на работните им задължения. Всички записи и документи на хартиен носител, съдържащи лични данни, са в заключени шкафове, ограничен достъп, достъпен само от упълномощен персонал. Данни са защитени чрез използването на средства за физически контрол на достъпа, като заключване на вратите и шкафовете .

5.2. Достъп се предоставя само на служителите, на които е пряко възложено това или на Гл.Счетоводител , на които той е необходим, за изпълнение на служебните им задължения, след оторизация.

5.3 .Достъп до личните данни на лицата, съдържащи се на технически носител има само обработващият лични данни, а в негово отсъствие и когато тези данни се отнасят до възнагражденията на лицата, достъп до тях има временно упълномощено от обработващият лични данни лице, комуто е известна паролата за достъп до файловете.

5.4. Личните данни се събират само с конкретна цел, за да подкрепят законните интереси на администратора на лични данни или до колкото е необходимо да се съобразят със законовите задължения на администратора на лични данни. Всеки тип данни се класифицира в съответствие с неговото предназначение и характер, и са защитени в съответствие с изискванията

5.5. Достъпът до регистрите е ограничен и се предоставя само на упълномощения персонал от отдел „Администрация“ или на Гл.счетоводител , в съответствие с принципа на „*Необходимост да знае*“.

5.6. Никое оправомощено или трето лице няма право на достъп до регистъра с личните данни на лицата, освен ако е изисквано по надлежен път от органи на надзора или на съдебната власт (Комисия за финансов надзор, съд, прокуратура, следствени органи и др.). Достъпът на тези органи до личните данни на лицата е правомерен.

5.6.1 Правомерен е и достъпът на ревизиращите държавни органи, надлежно легитимирали се със съответни документи – писмени разпорежданя на съответния орган, в които се посочва основанието, имената на лицата, като за целите на дейността им е необходимо да им се осигури достъп до кадровите досиета на персонала или клиентите.

5.7 При промени в статута на ДГ (преобразуване, ликвидация и други), налагачи прехвърляне на регистрите за лични данни от ДГ на друг администратор на лични данни, предаването на регистъра се извършва след разрешение на Комисията за защита на лични данни. Решението си за предоставяне или отказване достъп до лични данни за съветното лице администраторът съобщава на третите лица в 30-дневен срок от подаване на молбата, resp. искането.

6.Зашита на автоматизираните информационни системи и/или мрежи

6.1. Телекомуникации и отдалечен достъп.

Отдалечен достъп - Отдалечен достъп до вътрешни мрежи на ДГ ще бъде предоставен за оторизирани бизнес нужди, при поискване. Интернет достъп - на членовете на персонала може да бъде предоставен достъп до интернет, за да изпълняват служебните си задължения, но индивидуалният достъп може да бъде прекратен по всяко време по прещенка на ДГ. Цялата информация, получена чрез интернет трябва да бъде под съмнение, докато не бъде потвърдена от надеждни източници.

6.2. Защита от вируси.

ДГ създава и поддържа стандартни и сигурни конфигурации за всяка компютърна и мрежова платформа, с която оперира. Системният софтуер се контролира и се поддържа . Сканериране на компютърни вируси -хардуерът на ДГ трябва да работи и да бъде актуализиран с версии на одобрени антивирусни софтуер скрининг и вирусните подписи на компютрите да бъдат активирани. Потребителите не трябва да отказват автоматични софтуерни процеси, които актуализират вирусните подписи. Антивирусният софтуер скрининг трябва да се използва, за да сканира всички софтуери и файлове с данни, идващи от или до трети страни или други групи на ДГ . Членовете на екипа не трябва да избягват или да изключват сканиране на процесите, които биха могли да предизвикат предаването на компютърни вируси. Флопи дискове и други магнитни носители, използвани от зарazen компютър не трябва да се използват на друг компютър, докато вирусът не бъде успешно премахнат. Заразеният компютър също трябва да бъде незабавно изолиран от вътрешните мрежи. Потребителите не трябва да опитват да премахнат вируса, тъй като информационните технологии ще премахнат вирусите. Антивирусните логове трябва да се съхраняват в продължение на най-малко седем (7) дни.

6.3 При внедряване на нов програмен продукт за обработване на лични данни се извършва предварителна проверка на възможностите на продукта с оглед спазване изискванията на ЗЗЛД и Регламент (ЕС) 2016/679 и осигуряване максималната им защита от неправомерен достъп, загубване, повреждане или унищожаване

6.4. Копия/резервни копии за възстановяване;

Архивиране на информацията - Целта на ДГ е да поддържа наличността на информацията. Информацията, съдържаща лични данни трябва да бъде архивирана в съответствие със стандартите за архивиране на данни. Ако бъде необходимо, трябва да се инсталира или предостави техническа помощ за инсталирането на резервен хардуер. Всички архиви, съдържащи данни или поверителна информация за детската градина трябва да се съхранява с физически контрол на достъпа и трябва да се инвентаризира поне веднъж на тримесечие.

6.7 Процедури за унищожаване/заличаване/изтрягане на носители:
Данни, които вече не са необходими за целите на ДГ или за юридически цели, в съответствие с разпоредбите на чл. 25, ал. 1, т. 1 от ЗЗЛД, трябва да бъдат унищожени по безопасен начин чрез средства, като предиране, изгаряне или постоянно заличаване от електронните средства. Когато трета страна е ангажирана със съответен договор да провежда безопасни процеси по унищожаване от името на АЛД, за извършеното унищожаване на документи с лични данни трябва да се изиска надлежен протокол.

7. Криптографска защита

7.1. Криптирането се използва за защита на личните данни, които се предават от АЛД по електронен път или на преносими носители, когато такива данни се предават извън логически или физически контрол на АЛД.

Допустимата криптираща технология трябва да бъде стандартна технология, включително симетрично криптиращите технологии AES, 3DES, Blowfish, RSA, RC4, RC5, и IDEA.

8. Действия за защита на личните данни при аварии, произшествия и бедствия (пожар, наводнение и др.

Трябва да се следват процедурите за управление по време на такова събитие за защита на физическите и информационни активи, включително ангажиране на допълнителна сигурност на помещението и възстановяване на личните данни и други данни на ДДГ 43“Пинокио“ чрез извършване на редовно архивиране.

ПРЕДОСТАВЯНЕ НА ЛИЧНИТЕ ДАННИ

1. Всяко физическо лице има право на достъп до отнасящи се за него лични данни.

1.1 Правото на достъп се осъществява с писмено заявление до директора (*Приложение № 5*). Заявление може да бъде отправено и по електронен път по реда на ЗЗЛД, Закона за електронния документ и електронния подпис (ЗЕДЕП). Заявлението се отправя лично от физическото лице или от изрично упълномощено от него лице чрез нотариално заверено пълномощно. Заявлението съдържа:

- име, адрес и други данни за идентифициране на съответното физическо лице;
- описание на искането;
- предпочтата форма за предоставяне на информацията;
- подпис, дата на подаване на заявлението и адрес за кореспонденция.

1.1.1 Мястото , на който се приемат заявления за достъп и предоставяне на лични данни от регистрите е ДДГ 43“Пинокио“ – централна градска кабинет на ЗАС или на електронен адрес: pinochio_50@abv.bg

1.2. При подаване на заявление от упълномощено лице към заявлението се прилага и нотариално завереното пълномощно.

1.3. Информацията може да бъде предоставена под формата на устна или писмена справка или на преглед на данните от съответното физическо лице или от изрично упълномощено от него друго лице. Физическото лице може да поиска копие от обработваните лични данни на предочитан носител или предоставяне по електронен път, освен в случаите, когато това е забранено от закон. Директорът е длъжен да се съобрази с предочитаната от заявителя форма на предоставяне на информацията.

1.4. Директорът разглежда заявлението за предоставяне на пълна или частична информация, и се произнася в 14-дневен срок от неговото подаване, съответно 30-дневен, когато е необходимо повече време за събиране личните данни на лицето с оглед възможни затруднения в дейността на администриратора. Решението се съобщава писмено на заявителя лично срещу подпись или по пощата с обратна разписка

1.5. Директорът отказва достъп до лични данни, с мотивирано решение когато те не съществуват или предоставяното им е забранено със закон.. Отказът за предоставяне достъп може се обжалва от лицето пред посочения в писмoto орган и срок.

1.6. В случаите, когато при осъществяване правото на достъп на физическото лице, могат да се разкрият лични данни и за трето лице, директорът е длъжен да предостави на съответното физическо лице достъп до частта от тях, отнасяща се само за него.

2. Достъп до личните данни могат да имат :трети лица по силата на договор ,лица обработващи личните данни на предвидени по закон държавни органи – Министерство на образованието, Министерство на правосъдието ,РУО ,Община Варна ,а на чуждестранни физически и/или юридически лица, извън територията на Република България и Европейския съюз само след разрешение на КЗЛД. За тези действия физическите лица трябва предварително да бъдат уведомявани, преди да им се обработват личните данни.

3. Личните данни за лицата не се изнасят извън сградата на администратора. Никое длъжностно или трето лице няма право на достъп до личните данни от“РЕГИСТРИТЕ“ в ДД 43 Пинокио , освен ако същите

не са изискани по надлежен път от органи на съдебната власт (съд, прокуратура, следствени органи, МВР, НОИ, МОН). Достъпът на тези органи до личните данни на лицата е правомерен.

4.Правомерен е и достъпът на ревизиращите държавни органи, надлежно легитимирали се със съответни документи – писмени разпореждания на съветния орган, в които се посочва основанието, имената на лицата, като за целите на дейността им е необходимо да им се осигури достъп до кадровите досигта на персонала.

5.Не се изисква съгласие на лицето, ако обработването на неговите лични данни се извършва само от или под контрола на компетентен държавен орган за лични данни, свързани с извършване на престъпления, на административни нарушения и на непозволени увреждания. На такива лица се осигурява достъп до личните данни, като при необходимост им се осигуряват съответни условия за работа в помещение на ДГ

6.Лични данни от регистрите по чл. 2 могат да бъдат предоставяни в страни извън Европейския съюз само след спазване на законовите изисквания и получуване на необходимите разрешения от КЗЛД.

ОГРАНИЧАВАНЕ ОБРАБОТВАНЕТО НА ЛИЧНИ ДАННИ

1. Всяко физическо лице има право да изисква от администратора ограничаване обработването на относящи се за него лични данни, когато :

1.1 Точността на личните данни се оспорва от лицето, за срок, който позволява на администратора да провери точността на личните данни;

1.2 Обработването е неправомерно, но лицето не желае личните данни да бъдат изтрити, а изисква вместо това ограничаване на използването им;

1.3 Администраторът не се нуждае повече от личните данни за целите на обработването, но лицето ги изисква за установяването, упражняването или защитата на правни претенции;

1.4 Лицето е възразил срещу обработването в очакване на проверка дали законните основания на администратора имат преимущество пред интересите на субекта на данните.

2.Физическото лице изисква от администратора ограничаване обработването на отнасящи се за него лични данни ,чрез искане по образец „**Приложение 6**“

УНИЩОЖЕНИЕ НА ЛИЧНИ ДАННИ .

1. След постигане целта на обработване на личните данни когато вече не са необходими за детската градина или правни цели , преди прехвърлянето на контрола върху обработването, личните данни съдържащи се в Регистрите по т. 2 следва да бъдат унищожени по сигурен начин или прехвърлени на друг администратор на лични данни, съобразно изискванията на Закона за защита на личните данни , Регламент (ЕС) 2016/679 и при спазване на допулосочените процедури.

1.1Личните данни могат да бъдат унищожени по искане на Физическото лице изявено писмено - **Приложение 3**

2. Лични данни, съхранявани на електронен носител и сървъри трябва да бъдат унищожени чрез трайно изтриване, като презаписването на електронните средства или физическо унищожаване на средствата или сървъра. Лицето, което отговаря за този процес, е Директорът за всяко унищожаване се издава нарочна заповед и се съставя последващ надлежен протокол .Трета страна, ангажирана въз основа на склучен договор да провежда безопасни процеси по унищожаване от името на администратора на лични данни, е длъжна да предостави Протокол за извършено унищожаване на лични данни.

3. Документите на хартиен носител, съдържащи лични данни трябва предпазливо да бъдат предиранни или изгорени когато периодът за съхранение е изтекъл. Лицето, което отговаря за този процес, е Директорът за всяко унищожаване се издава нарочна заповед и се съставя последващ надлежен протокол.

4. Процедура за прехвърляне на лични данни на друг администратор на лични данни съгласно чл. 25 от Закона за защита на личните данни. Всички трансфери на данни ще се извършва с помошта на защитени средства, включително криптиране или виртуална частна мрежка.

5. След постигане целта на обработване на личните данни съхранението на тези лични данни е допустимо само в предвидените в закон случаи.

САНКЦИИ И ОТГОВОРНОСТИ ПРИ НАРУШВАНЕ НА ПРАВИЛАТА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

1. За неизпълнение на задълженията, вменини на съответните оправомощени лица по тази инструкция, по ЗЗЛД и по Регламент (ЕС) 2016/679, след разследване се налагат дисциплинарни наказания по решение на директора на ДГ включително и уволнение

2. Когато неизпълнението на съответното задължение е констатирано и установено от надлежен орган – се налага предвиденото в ЗЗЛД административно наказание.

3. Освен оповестените изисквани от закона, всички трети лица, обработващи данните, които имат достъп до лични данни, се изисква да подпишат споразумение за обработка на данни и да спазват строги задължения за поверителност.

ПРЕХОДНИ И ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§ 1. Настоящата инструкция е задължителна за всички учители и служители на ДГ 43 “Пинокио“, доколкото те участват в обработването на личните данни по горните регистри, и други лица, които имат постоянен или временен достъп до лични данни от всички регистри.

§ 2. Контрол по изпълнението на настоящата инструкция се осъществява от Директора на Детската градина

§ 3. Изменения и допълнения на тази инструкция се правят по реда на издаването и утвърждаването й.

§ 4. Тази инструкция влиза в сила от 01.01.2020 г.

§ 5. Тази инструкция е утвърдена от Директора на ДГ със Заповед №108/23.12.2019 г.

ПРИЛОЖЕНИЕ 1

ДЕКЛАРАЦИЯ

Долуподписанит/ата ЕГН:

на длъжност в ДГ 43“Тинокио“

ДЕКЛАРИРАМ:

Съгласен/а съм ДГ 43“Тинокио“ (администратор на лични данни) да обработва личните ми данни, съгласно изискванията на Закона за защита на личните данни и Регламент (ЕС) 2016/679.

Запознат/а съм с:

- целта и средствата на обработка на личните данни;
- доброволния характер на предоставянето на данните и последиците от отказа за предоставянето им;
- правото на достъп, на коригиране и на изтриване на съхранените данни;
- получателите или категориите получатели, на които могат да бъдат разкрити данните.

Дата:
гр.

ПРИЛОЖЕНИЕ 2

ИСКАНЕ ЗА КОРИГИРАНЕ(АКТУАЛИЗАЦИЯ) НА ЛИЧНИ ДАННИ

Долуподписаният, - субект на лични данни,
след като се уверих в неточността на съхраняваните при администратора лични данни, с настоящата молба моля
да бъдат допълнени/ коригирани следните лични данни:
.....
.....
.....

Моля, данните да бъдат коригирани в законоустановения срок.

Уведомен съм за целта, за която данните ще бъдат използвани, а
именно.....
дата

С уважение!

Три имена, подпись

Получил /три имена/:

дата подпись

ПРИЛОЖЕНИЕ 3

ИСКАНЕ ЗА ИЗТРИВАНЕ НА ЛИЧНИ ДАННИ

Долуподписаният, , като субект на лични данни, обработени и съхранявани от ДГ 43 „Пинокио“ . - администратор на лични данни, с настоящата декларация заявявам, че желая свързаните с мен лични данни да бъдат изтрити без ненужно забавяне, по следната причина:
.....

(причината трябва да бъде една от посочените в чл. 17 от Общий регламент).

Моля, да се уведомят всички администратори и обработващи личните ми данни, че съм поискал изтриване на личните ми данни, включително на всички връзки, копия или реплики на тези лични данни.

Дата

С уважение!

Три имена /изписват се собственоръчно/

Подпись

Получил /три имена/:

дата подпись

ПРИЛОЖЕНИЕ 4

ДЕКЛАРАЦИЯ - СЪГЛАСИЕ

С настоящата декларация долуподписаният:

Три имена: ЕГН:

Адрес: Телефонен номер:

Имейл: В качеството си на родител/настойник на:

ИНФОРМАЦИЯ ЗА ДЕТЕТО:

Три имена: от група

ЕГН: Дата на раждане: Месторождение.....

.Адрес:

ДЕКЛАРИРАМ :

Съгласен/а съм ДГ 43“Пинокио“ да обработва личните ми данни и тези на малолетно / нещънолетното ми дете, съгласно изискванията на Регламент (ЕС) 2016/679 на Европейския парламент и Съвета от 27.04.2016 г ,които предоставям във връзка с кандидатстване и обучение в ДГ 43“Пинокио“

Информиран/ а, че предоставените от мен лични данни ще бъдат използвани само за целите на работа на ДГ 43“Пинокио“ и изискванията на нормативните актове, регламентиращи дейността на ДГ 43“Пинокио“

Запознат/а съм с:

- цепта и средствата на обработване на личните ми данни и тези на малолетно/ нещънолетното ми дете/на детето, чийто настойник съм.
- правата ми по чл. 15 -22 от Регламент 2016/679 на дъстъп, коригиране, изтриване, ограничаване на обработването, както и правото ми на преводимост на данните и на възражение за обработване на на съхранените данни.
- Запознат съм, че личните данни ще се съхраняват по следния начин: на хартиен или електронен носител . , според законовите изисквания за защита на данните.

С настоящата декларация, доброволно се съгласявам мойте лични данни и тези на детето ми да бъдат обработвани , в това число и да бъдат съхранявани при спазване на разпоредбите на Регламент 2016/679, Закона за защита на личните данни и подзаконовите актове по прилагането му.

Запознат/а съм с възможността да отгеля това съгласие за обработване на лични данни на мен и детето частично или изцяло по всяко време, за което следва да уведомя администратора по следния начин: писмено или усто .Запознат съм и с последващите от това мое действие последици.

Дата

Декларатор:.....

Град

ПРИЛОЖЕНИЕ 5

ИСКАНЕ

За ограничаване обработването на лични данни

Долуподписаният, , в качеството ми на субект на лични данни, обработвани и съхранявани при ДГ 43 „Пинокио (администратор на лични данни) с настоящото искане Ви информирам, че желая обработването на личните ми данни да бъде ограничено по следната причина:
.....
.....

Моля всички засегнати трети страни да бъдат уведомени за ограничаването на обработването на личните данни.

Дата:

Три имена:

Подпись:

Получил /три имени/:

дата

подпись

