Детска градина №91 „Слънчев кът“
Столична Община, р-н „Подуяне“
ул. „Поручик Георги Кюмюрджиев“ №25, ж.к. „Левски Г“, гр. София, 1836
телефон: +359 879 06 54 25; e-mail: info-2219888@edu.mon.bg

ВЪТРЕШНИ ПРАВИЛА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

НА ДГ №91 „Слънчев кът“

I. ОБЩИ ПОЛОЖЕНИЯ И НОРМАТИВНА ОСНОВА

Чл. 1. (1) Настоящите правила уреждат принципите, организацията, отговорностите, техническите и организационните мерки за законосъобразно обработване на лични данни от ДГ №91 „Слънчев кът“ (наричана по-долу „детската градина“).

(2) Прилагат се за основната сграда, филиалите и останалите обекти, в които детската градина осъществява дейност, както и за работа извън тях със служебна информация.

Чл. 2. Правилата се основават на Регламент (ЕС) 2016/679 (ОРЗД/GDPR), Закона за защита на личните данни, Закона за предучилищното и училищното образование, приложимите подзаконови актове, трудовото и архивното законодателство и относимите актове за здравно обслужване и приобщаващо образование.

Чл. 3. Детската градина е администратор на лични данни за обработванията, чиито цели и средства определя самостоятелно. Когато обработването се извършва в централизирана система или съвместно с друга институция, ролите и отговорностите се установяват за конкретната дейност.

Чл. 4. Правилата са задължителни за директора, заместник-директора, педагогическите специалисти, медицинските специалисти, административния, помощния и обслужващия персонал, както и за лица с разрешен достъп до данните.

II. ПРИНЦИПИ И ПРАВНИ ОСНОВАНИЯ

Чл. 5. Всяко обработване се извършва законосъобразно, добросъвестно и прозрачно; за конкретни цели; с минимален обем данни; при точност и актуалност; с ограничени срокове на съхранение; при цялостност и поверителност и с възможност за доказване на съответствието (отчетност).

Чл. 6. (1) За всяка дейност се определя конкретно правно основание по чл. 6, пар. 1 ОРЗД: законово задължение, задача от обществен интерес/упражняване на официални правомощия, договор, жизненоважни интереси или друго приложимо основание.

(2) Съгласието се използва само когато е действително свободно, конкретно, информирано и недвусмислено, и може да бъде оттеглено без неблагоприятни последици.

Чл. 7. Обработването на здравни данни, данни за специални образователни потребности и други специални категории данни изисква едновременно основание по чл. 6 и приложимо изключение по чл. 9, пар. 2 ОРЗД. Достъпът до тези данни е особено ограничен.

Чл. 8. Не се изисква съгласие за задължителна по закон обработка, включително за водене на нормативно установената документация. Липсата на съгласие за незадължителна публикация на снимка не може да препятства приемането, обучението или участието на детето в дейности.

III. КАТЕГОРИИ ЛИЦА, ДАННИ И ЦЕЛИ

Чл. 9. Обработват се данни на: деца; родители, настойници и други законни представители; лица, оправомощени да вземат дете; настоящи и бивши служители и кандидати за работа; посетители, изпълнители и представители на институции.

Чл. 10. За децата могат да се обработват имена, ЕГН или друг идентификатор, адрес и контактна информация, данни за прием, посещаемост, обучение и развитие, информация за законните представители, необходими здравни сведения, данни за подкрепа за личностно развитие и други данни, които са нормативно изискуеми.

Чл. 11. За родителите и упълномощените лица се обработват идентификационни и контактни данни, данни за родителски права, представителство и изрично дадени разрешения; ЕГН и данни за месторабота се събират само при конкретно установена необходимост и правно основание.

Чл. 12. За служителите и кандидатите се обработват данни за подбор и квалификация, трудово правоотношение, възнаграждения и осигуряване, банкова сметка, отпуски, оценяване, медицинска пригодност в допустимия обем и други данни съгласно нормативните задължения.

Чл. 13. Целите включват организация и провеждане на предучилищно образование, здравни грижи, безопасност, приобщаващо образование, административно обслужване, кадрово и финансово управление, взаимодействие със законни представители, институционална отчетност и защита на законни права.

IV. ОРГАНИЗАЦИЯ И ОТГОВОРНОСТИ

Чл. 14. (1) Директорът определя организационните мерки, правата на достъп, лицата с отговорности по сигурността и условията за работа с външни изпълнители.

(2) При изпълнение на законовите критерии се определя длъжностно лице по защита на данните (ДЛЗД) с гарантирана независимост и без конфликт на интереси; осигурява се публикуване на данните за контакт и изпълнение на приложимите задължения за уведомяване на КЗЛД. Преди утвърждаването се проверява приложимостта на специалните указания на КЗЛД за образователни институции.

Чл. 15. ДЛЗД, когато е определено, консултира администратора и служителите, наблюдава съответствието, съдейства за оценките на въздействието и е контактна точка за надзорния орган и субектите на данни. ДЛЗД не взема управленските решения вместо администратора.

Чл. 16. Всеки служител обработва само данните, които са необходими за възложените му функции, не предоставя неразрешен достъп, не използва служебна информация за лични цели и съобщава незабавно за предполагаеми инциденти.

Чл. 17. Предоставянето на достъп се документира по длъжности и конкретни системи. При промяна на длъжност, продължително отсъствие или прекратяване на правоотношение достъпът се преглежда, ограничава или прекратява своевременно.

V. ПРАВИЛА ЗА РАБОТА С ДАННИ НА ДЕЦА И РОДИТЕЛИ

Чл. 18. Детските досиета и документи се поддържат в определени помещения и служебни системи; забранява се оставянето им без надзор на достъпни места, както и предоставянето им за преглед на други родители.

Чл. 19. Информация за дете се предоставя на негов законен представител след необходимата проверка на самоличността и правото му да получи конкретната информация. При спор относно родителски права, ограничителни мерки или съдебни актове се проверяват представените актуални документи и се прилага относимото право.

Чл. 20. Данни за здравето, алергии, специални потребности, психологична и логопедична подкрепа се съобщават само на лицата, за които това е необходимо по служба; в общи групови чатове, информационни табла и публични публикации не се разкрива индивидуална чувствителна информация.

Чл. 21. Списъци за предаване на деца, режими на хранене, лекарства или особености на грижата се изготвят в минимално необходимия обем и се пазят извън достъпа на посетители. Не се изписват диагнози върху общодостъпни табла.

Чл. 22. При предаване на дете на упълномощено лице се обработват само данните, нужни за установяване на право за получаване; копия от лични документи не се задържат без отделно правно основание.

VI. СНИМКИ, ВИДЕО, СЪБИТИЯ И ПУБЛИКАЦИИ

Чл. 23. Публикуването на разпознаваеми снимки и видеозаписи на деца на интернет страница, в социални мрежи, рекламни материали или публични презентации се допуска след определяне на подходящо правно основание, цел, канали, срокове и предоставяне на прозрачна информация. Когато основанието е съгласие, то се документира отделно и може да бъде оттеглено.

Чл. 24. Съгласието за публични снимки/видео не се обвързва с участие в образователна дейност. Предпочитат се групови кадри, които не разкриват имена, медицински данни, индивидуални затруднения или други ненужни подробности. При липса на основание детето не се публикува или се използва подходящо обезличаване.

Чл. 25. При тържества, посещения на театри и екскурзии детската градина информира родителите за предвиденото документиране и публикуване. Служителите не изпращат снимки на деца на свои лични профили и не използват лични облачни хранилища за служебни материали без изрично разрешение.

Чл. 26. Родителите и посетителите се информират за необходимостта да зачитат личния живот на останалите деца при собствено заснемане. Детската градина не може да гарантира поведението на всички присъстващи, но определя правила за събитията, които организира.

Чл. 27. Видеонаблюдение, ако е въведено, се урежда с отделна процедура, включително цели, правно основание, обхват на камерите, достъп, информация, срокове за съхранение и преценка за въздействие. Не се допуска автоматично предположение, че видеонаблюдение е разрешено във всички помещения; съобразяват се указанията и практиката на КЗЛД.

VII. ЕЛЕКТРОННИ СИСТЕМИ И КОМУНИКАЦИЯ

Чл. 28. Данни в НЕИСПУО и други нормативно или договорно определени системи се въвеждат само от оправомощени лица чрез индивидуални профили. Данните се проверяват за точност и се поддържа проследимост на операциите, когато системата позволява.

Чл. 29. Служебната електронна поща е предпочитаният канал за изпращане на документи с лични данни; получателите и прикачените файлове се проверяват преди изпращане. При масови съобщения се използва скриване на адреси (BCC), когато не е необходимо получателите да се виждат един друг.

Чл. 30. Не се допуска изпращане на ЕГН, здравни данни, оценки за развитие или копия на документи чрез неразрешени общи чатове. При необходимост се използват служебно одобрени защитени канали и ограничен кръг получатели.

Чл. 31. Служителите използват силни индивидуални пароли, двуфакторна защита при наличност, автоматично заключване, актуализирани устройства и антивирусна защита. Забраняват се споделяне на пароли, използване на чужд профил и съхранение на служебни файлове върху неразрешени лични носители.

Чл. 32. Печатните копия се вземат веднага от принтера; преносими носители се криптират, когато е подходящо; архиви и резервни копия се поддържат при определени права на достъп и се проверява възможността за възстановяване.

Чл. 33. Използването на външни облачни услуги, приложения с изкуствен интелект и интернет платформи за обработване на лични данни на деца и персонал се допуска само след предварително одобрение, оценка на риска, правното основание и условията на доставчика. Без такова одобрение служителите не въвеждат лични данни или поверителни документи в публични приложения.

VIII. ПРЕДОСТАВЯНЕ НА ДАННИ И ВЪНШНИ ОБРАБОТВАЩИ

Чл. 34. Данни се предоставят на компетентни държавни и общински органи само при установена законова компетентност и в необходимия обем. Исканията се документират и проверяват преди изпълнение.

Чл. 35. С доставчици, които обработват данни от името на детската градина, се сключва договор или друг правен акт с необходимите клаузи по чл. 28 ОРЗД. Определят се предметът и срокът, видовете данни, задълженията за поверителност, мерките за сигурност, подизпълнителите, съдействието при искания и инциденти, връщането или изтриването на данните.

Чл. 36. Предаване на данни извън Европейското икономическо пространство се допуска само при спазване на глава V ОРЗД и след предварителна преценка на използваната платформа/услуга.

IX. СРОКОВЕ ЗА СЪХРАНЕНИЕ И УНИЩОЖАВАНЕ

Чл. 37. За всяка категория документи се прилага срок, предвиден в действащата нормативна уредба, номенклатурата/сроковете на институцията или документираната необходимост. Сроковете не се определят произволно и се включват в регистъра на дейностите по обработване или приложение към него.

Чл. 38. След изтичане на срока документите се унищожават по начин, който предотвратява възстановяване, или се предават за архивиране, когато законът го изисква. Унищожаването на хартиени документи се удостоверява с протокол, а електронните данни се изтриват сигурно, като се отчита цикълът на резервните копия.

Чл. 39. При висящ правен спор, проверка или законово изискване за запазване унищожаването се спира само за относимите данни и за необходимия период.

X. ПРАВА НА СУБЕКТИТЕ И РЕД ЗА ИСКАНИЯ

Чл. 40. Субектите имат права на информация, достъп, коригиране, изтриване, ограничаване, възражение и, когато е приложимо, преносимост. Правата не са абсолютни: за всеки случай се проверяват правното основание, законовите задължения и правата на други лица.

Чл. 41. Искания се приемат на официалния електронен адрес, на място или по друг достъпен канал. Администраторът може при основателни съмнения да поиска допълнителна информация за потвърждение на самоличността, без да събира прекомерни данни.

Чл. 42. Отговор се предоставя без ненужно забавяне, по правило до един месец от получаване на искането. При сложност или множество искания срокът може да бъде удължен с още два месеца при уведомяване за причините в първоначалния едномесечен срок, съгласно чл. 12 ОРЗД.

Чл. 43. Отказът или ограничаването на право се мотивира и включва информация за възможността за жалба до Комисията за защита на личните данни и съдебна защита. Исканията и отговорите се документират в защитен регистър.

XI. НАРУШЕНИЯ НА СИГУРНОСТТА НА ЛИЧНИТЕ ДАННИ

Чл. 44. Нарушение е събитие, довело до случайно или неправомерно унищожаване, загуба, изменение, неразрешено разкриване или достъп до данни: напр. изпратено писмо до погрешен адресат, загубен носител, неправомерно публикувана снимка, компрометиран профил.

Чл. 45. Служителят незабавно уведомява директора и определеното контактно лице/ДЛЗД, като не прикрива инцидента и не изтрива доказателства. Своевременно се предприемат мерки за ограничаване: оттегляне на съобщение, смяна на парола, блокиране на профил, изтегляне на публикация и други подходящи действия.

Чл. 46. Директорът организира оценка на вероятния риск за правата и свободите на засегнатите лица. При наличие на риск уведомява КЗЛД без ненужно забавяне и когато е осъществимо, не по-късно от 72 часа след узнаване. При вероятен висок риск засегнатите лица се уведомяват без ненужно забавяне, освен ако е приложимо законово изключение.

Чл. 47. Всички нарушения, включително случаите без уведомяване до КЗЛД, се документират с фактите, последиците, оценката на риска, взетите мерки, решенията и сроковете. Периодично се анализират причините и необходимите превантивни действия.

XII. ОЦЕНКА НА РИСКА, ОБУЧЕНИЕ И КОНТРОЛ

Чл. 48. При въвеждане на нова система, видеонаблюдение, мащабно обработване на чувствителни данни или друга нова дейност се извършва предварителна оценка на риска; когато са налице условията по чл. 35 ОРЗД, се извършва оценка на въздействието върху защитата на данните.

Чл. 49. Най-малко веднъж годишно се преглеждат правата за достъп, регистрите, сроковете за съхранение, сигурността на устройствата, договорите с обработващи и образците за информиране/съгласие. При съществена промяна прегледът се извършва незабавно.

Чл. 50. При постъпване и периодично служителите се запознават с правилата и получават практическо обучение. Подписват декларация за поверителност или аналогично задължение; задължението за опазване на защитената информация продължава и след прекратяване на правоотношението, когато законът я изисква.

Чл. 51. Директорът упражнява контрол и предприема корективни мерки. Нарушенията се разглеждат съгласно приложимия правен ред; дисциплинарната отговорност не изключва други предвидени в закона последици.

Директор: _____
/Таня Кечева/

РАЙОН ПОДУЯНЕ ДГ № 91 СОФИЯ