|  |  |
| --- | --- |
| **ОБЩИНА РАДНЕВО**  **6260 Раднево, ул. "Митьо Станев" №1, тел.: 0417/8-20-72, факс: 0417/8-22-80,**  **е- mail:** [**obshtina@obshtina.radnevo.net**](mailto:obshtina@obshtina.radnevo.net)**,**  [**www.radnevo.acstre.com**](http://www.radnevo.acstre.com)  **GDPR *ПОЛИТИКА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ*** |  |

**УТВЪРЖДАВАМ,**

**ДИРЕКТОР НА**

**ДГ „………………..“:**

**………………………….**

**ВЪТРЕШНИ ПРАВИЛА**

**ЗА ИЗВЪРШВАНЕ НА ОЦЕНКА НА ВЪЗДЕЙСТВИЕТО ВЪРХУ ЛИЧНИТЕ ДАННИ**

# ОБЩИ ПОЛОЖЕНИЯ.

## Цел и обхват на документа.

**Чл.1.** Този документ цели да осигури изпълнението на задължението на Детска градина „............................“ да извършва оценка на въздействието върху личните данни.

**Чл.2.** Описаната в този документ процедура съдържа указание за случаите, в които е задължително извършването на оценка на въздействието и методологията за оценка на въздействието.

**Чл.3.** Оценката на въздействието върху защитата на данните (ОВЗД) е процес, който позволява на Детска градина „............................“ да прецени необходимостта и пропорционалността на конкретно приложение, решение, модул или процес от гледна точка на защитата на личните данни; да се определят рисковете за защита на данните, свързани с процеса; да се реши какви допълнителни технически и организационни мерки за сигурност са необходими и подходящи за спазване на нормативните задължения към обработката на лични данни.

## Адресати на документа.

**Чл.4.** Адресати на описаната в този документ процедура са служителите в Детска градина „............................“, които извършват дейности по обработка на личните данни.

**Чл.5.** Отговорно лице за актуализирането и прилагането на настоящата процедура е длъжностното лице по защита на данните.

*Понятия*

**Чл.6.** В настоящия документ, понятията са използвани в смисъла, определен от Европейския комитет по защита на данните (Работната група по чл. 29)[[1]](#footnote-1), както следва:

1. *Оценка на въздействието върху личните данни* е процес, чиято цел е да опише обработването, да оцени неговата необходимост и пропорционалност и да спомогне за управлението на рисковете за правата и свободите на физическите лица, произтичащи от обработването на лични данни, като ги оцени и определи мерки за справяне с тези рискове;
2. *Риск* е сценарий, описващ дадено събитие и неговите последици, оценени от гледна точка на тяхната тежест и вероятност;
3. *Управление на рисковете* представлява координирани дейности за ръководенето и контролирането на дадена организация във връзка с риска.
4. **ИЗИСКВАНЕ ЗА ОЦЕНКА НА ВЪЗДЕЙСТВИЕТО.**

**Чл.7**. **/1/** Детска градина „............................“ извършва ОВЗД за процеси по обработка с „висок риск“ за правата и свободите на субектите на данни, особено когато се използват нови технологии.

**/2/** ОВЗД представлява по същество оценка на риска, която трябва да вземе предвид естеството, обхвата, контекста и целите на обработката на лични данни и се извършва преди началото на обработката.

**/3/** Независимо дали процесът /технологията/ е създаден от Детска градина „............................“ или е закупен или лицензиран от трета страна, ОВЗД трябва да започне възможно най-рано при възлагането или проектирането на процеса, дори ако някои от операциите все още не са сигурни.

**Чл.8.** ОВЗД се извършва задължително в случаите, когато:

а) обработката включва систематична оценка на личните аспекти на физическото лице;

б) се извършва мащабно обработване на специални категории данни;

в) се извършва систематично мащабно наблюдение на публично достъпна зона,

при прилагане на дерогациите на Общия регламент за защита на личните данни.

**Чл. 9. /1/** Когато извършването на ОВЗД не е задължително,се извършва преценка за всеки конкретен случай на обработка.

**/2/** Преценката дали е необходима ОВЗД се извършва преди:

а) въвеждане на нов процес, система или технология, включващи обработката

на лични данни; или

б) извършване на значителни промени във всички съществуващи процеси,

системи или технологии за обработка на лични данни.

**/3**/ При преценката по ал.1 се вземат предвид различни фактори, които е вероятно да увеличат риска във връзка с даден процес на обработка и следователно изискват ОВЗД. Такива фактори включват, но не се ограничават до дейности като:

а) оценка или точкуване, включително профилиране и прогнозиране;

б)автоматизирано вземане на решения с правни последици или подобни сериозни последици;

в) систематично наблюдение;

г)обработка на чувствителни данни или данни от изключително лично естество;

д) търсене на съвпадение или съчетаване на набори от данни;

е) обработка на данни относно уязвими субекти на данни;

ж)иновативно използване или прилагане на нови технологични или организационни решения;

з) когато операциите по обработването сами по себе си „възпрепятстват субектите на данни да упражняват дадено право или да използват някоя услуга или договор“.

**/4/** Посоченият в ал.3 списък може да бъде допълван и актуализиран в съответствие със списък с вида операции по обработка, които изискват ОВЗД, изготвен от Комисията за защита на личните данни, ако и когато списъкът бъде публикуван.

**/5/** Преценката относно необходимостта от извършване на ОВЗД се извършва от Директора на Детска градина „............................“

/**6**/ Длъжностното лице по защита на личните данни предоставя становище относно необходимостта от извършване на ОВЗД.

**/7**/ Ако лицето по ал. 5 не е съгласно със становището на длъжностното лице по защита на личните данни, то следва да се обоснове в писмен вид защо становището не е взето предвид.

1. **ИЗВЪРШВАНЕ НА ОЦЕНКА НА ВЪЗДЕЙСТВИЕТО.**

**Чл.10.** /1/ Всички ОВЗД се извършват 6 месеца и при всички случаи най-малко 2 месеца преди да започне обработката.

/2/ За извършването на ОВЗД се прилага Методология за оценка на въздействието върху личните данни /***Приложение № 1*** /. По преценка на длъжностното лице по защита на личните данни Методологията може да бъде променяна, така, че да се улесни извършването на конкретна оценка на въздействието.

**/3/** Методологията се изпраща на всички служители, които трябва да бъдат включени в зависимост от естеството на процеса. Участващите служители от Детска градина „............................“ се определят от длъжностното лице по защита на данните.

**/4/** Със заповед на Директора на Детска градина „............................“ се определя комисия от служители, която на базата на представената информация, съгласно ал.3 и ал.4 изготвят оценка на въздействието.

**/5/** Комисията по ал. 4 работи под ръководството на длъжностното лице по защита на данните в Детска градина „............................“, което прави оценка дали ОВЗД е направена правилно и дали заключенията от нея показват спазване на законодателството за защита на личните данни.

1. **ОСОБЕНИ СЛУЧАИ.**

**Чл.11. /1/** При извършването на ОВЗД следва да бъдат съобразени няколко особени случаи на обработка на лични данни, като при необходимост може да се потърси съвет от независими експерти.

**/2/** В случаите, когато няколко процеса са сходни по отношение на обстоятелствата и представения риск (например, когато се използва подобна технология за събиране на същите данни за същите цели), една ОВЗД може да оцени всички тези процеси.

**/3/** В случаите когато Детска градина „............................“ планира да извършва обработка на лични данни в сътрудничество с един или повече други администратори на данни като съвместни администратори, трябва да се определят съответните си задължения във връзка с ОВЗД.

**/4/** В случаите когато обработката ще се извършва изцяло или частично от обработващи, Детска градина „............................“ осигурява необходимото съдействие от тези обработващи при извършването на ОВЗД.

**/5/** В случаите на внедряване на нов технологичен продукт, като например нова

програма или приложение за обработка на данни, Детска градина „............................“ иска от доставчика копие от ОВЗД, извършена от доставчика.

1. **ОТГОВОРНИ ЛИЦА И КОНСУЛТИРАНЕ С НАДЗОРНИЯ ОРГАН.**

**Чл.12.** Комисията по чл.10, ал.4 отговаря за провеждането на ОВЗД.

**Чл.13. /1/** Когато процесът остава „високорисков“ (т.е. когато остатъчните рискове са високи), Детска градина „............................“ извършва предварителна консултация с Комисията за защита на личните данни.

**/2/** Не се допуска обработване на лични данни, обхванати от съответната ОВЗД, до приключване на консултацията.

**/3/** За целите на консултирането Детска градина „............................“ предоставя на КЗЛД минимум следната информация:

а) съответните отговорности на администратора, съвместните администратори и обработващите, участващи в обработката, ако има такива;

б) целите и средствата на планираната обработка;

в) мерките и предпазните мерки, предвидени за защита на правата и свободите на субектите на данни;

г) данните за връзка;

д) копие от завършената ОВЗД; и

е) всяка друга информация, поискана от надзорния орган.

**/4/** Предварителната консултация с Комисията за защита на личните данни се извършва от длъжностното лице по защита на данните.

1. **ПРЕХОДНИ И ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ.**

**§. 1** Настоящите Вътрешни правила за оценка на въздействието влизат в сила от деня на утвърждаването им.

**§.2.** Настоящите Вътрешни правила се преглеждат веднъж годишно и при необходимост се актуализират.

*Приложение №1*

**МЕТОДОЛОГИЯ**

**ЗА ИЗВЪРШВАНЕ НА ОЦЕНКА НА ВЪЗДЕЙСТВИТЕ ВЪРХУ ЛИЧНИТЕ ДАННИ.**

Необходимост от ОВЗД

|  |
| --- |
| Посочете какъв вид обработка ще извършвате. Аргументирайте необходимостта от извършване на ОВЗД |
|  |

Описание на процеса по обработка

|  |
| --- |
| Отговорни лица |

Моля, попълнете таблицата, като отговорите на поставените въпроси.

|  |  |
| --- | --- |
| **Въпроси** | **Отговори** |
| Кое лице определи необходимостта от извършване на дейността по обработка |  |
| Коя организация ще информира субекта на данните за процесите по обработка? |  |
| Коя организация е отговорна за определянето на основните аспекти на процеса по обработка? | Обхват на данните –………………………………  Категории субекти на данни– ………………  Разкриване на данни –……………………………  Права на субектите –……………………………..  Съхраняване и унищожаване на данни –……………………………………………………  Място на съхранение на данните–…………………………  Сигурност на данните –……………………………………………….., |

|  |
| --- |
| Естеството на процеса по обработка |

Моля, попълнете таблицата, като отговорите на поставените въпроси.

|  |  |
| --- | --- |
| Въпроси | Отговори |
| Как се извършва процесът на обработка на личните данни? |  |
| От кого се получават личните данни? | От самия субект на данните  От трета страна |
| Как се събират данните (попълва се само, когато данните се получават директно от субекта)? | Чрез попълване на документ на хартиен носител  Чрез попълване на електронен документ  Автоматично от информационна система (посочете конкретната технология, напр. бисквитки…………………………………………………………….  Чрез технология за следене във виртуална среда (посочете конкретната технология, напр. периодично заснемане на работния екран на компютъра)……………………………………………………………  Чрез наблюдение в традиционна среда (посочете начина на наблюдение напр. видеонаблюдение или звукозапис)  Друг начин (посочете начина)……………………………………………………… |
| Как се получават данните (попълва се само, когато данните **НЕ** се получават директно от субекта)? | Осигурен е достъп от разстояние  Получават се чрез пренос на данни по електронен път (посочете начина на пренасяне)…………………………………………………………….  Получават се на хартиен носител (посочете конкретната технология, напр. периодично заснемане на работния екран на компютъра)……………………………………………………………  Друг начин (посочете начина)……………………………………………………………….. |
| Как може да бъде индивидуализирано лицето, чрез използване на данните? | Данните позволяват идентифициране на лицето и установяване на правно индивидуализиращите го данни (свързване с гражданската му самоличност);  Данните позволяват идентифициране на лицето, но не и свързване с гражданската му самоличност; |
| Каква физическа и техническа инфраструктура се използва за обработката на данните? |  |

|  |
| --- |
| Обхват на обработката |

Моля, попълнете таблицата, като отговорите на поставените въпроси.

|  |  |
| --- | --- |
| Въпроси | Отговори |
| Какви категории лични данни се обработват? |  |
| Обработват ли се специални категории лични данни? | Обработват се чувствителни лични данни (посочете какви)…………………………………………………………………………  Обработват се данни относно присъди и наказания |
| Колко често се извършва обработката? | Периодично (посочете интервалите или условията, които определят периодичността)……………………………………………………………..  Постоянно |
| Колко субекта на данни са засегнати? |  |
| В каква географска област се извършва обработката? |  |

Консултация със заинтересованите лица

|  |
| --- |
| Консултации с членове на организацията |

Моля, попълнете таблицата, като отговорите на поставените въпроси.

|  |  |
| --- | --- |
| Въпроси | Отговори |
| Има ли лица, с които следва да бъде обсъдена оценката на въздействието? |  |
| Как е извършено обсъждането? |  |
| До каква степен е съобразено мнението им при извършване на оценката? |  |

|  |
| --- |
| Консултации с обработващи личните данни |

Моля, попълнете таблицата, като отговорите на поставените въпроси.

|  |  |
| --- | --- |
| Въпроси | Отговори |
| Имали обработващи, които са включени в процеса на изготвяне на ОВЗД? |  |
| Как е извършено обсъждането? |  |
| До каква степен е съобразено мнението им при извършване на оценката? |  |

|  |
| --- |
| Консултации с компетентни органи |

Моля, попълнете таблицата, като отговорите на поставените въпроси.

|  |  |
| --- | --- |
| Въпроси | Отговори |
| Има ли държавни органи или органи на местното самоуправление, с които следва да бъде обсъдена оценката на въздействието? |  |
| Как е извършено обсъждането? |  |
| До каква степен е съобразено мнението им при извършване на оценката? |  |

|  |
| --- |
| Консултации със субектите на данните |

Моля, попълнете таблицата, като отговорите на поставените въпроси.

|  |  |
| --- | --- |
| Въпроси | Отговори |
| Включени ли са субекти на данните в процеса на изготвяне на ОВЗД? |  |
| Как е извършено обсъждането? |  |
| До каква степен е съобразено мнението им при извършване на оценката? |  |

|  |
| --- |
| Консултации с външни експерти |

Моля, попълнете таблицата, като отговорите на поставените въпроси.

|  |  |
| --- | --- |
| Въпроси | Отговори |
| Извършена ли е консултация с външни експерти?  Ако да – експерти в каква област за избрани? |  |
| Как е извършено обсъждането? |  |
| До каква степен е съобразено мнението им при извършване на оценката? |  |

Оценка на необходимостта и пропорционалността

Принципи за защита на личните данни

|  |
| --- |
| Цели на обработката |

Моля, попълнете таблицата, като отговорите на поставените въпроси.

|  |  |
| --- | --- |
| Въпроси | Отговори |
| С каква цел се извършва обработката? |  |
| Каква е ползата за организацията от извършването на обработката? |  |
| Постигат ли се поставените цели чрез дейността по обработка? |  |
| Има ли друга дейност, чрез която могат да бъдат постигнати поставените цели? |  |
| Как обработката засяга субектите на данни? |  |
| Планира ли се използването на данните за различна цел в следващите 12-18 месеца? |  |
| Има ли осигурени мерки, които да не позволяват използването на данните за цел различна от посочената?  Ако да–посочете всички мерки |  |

|  |
| --- |
| Законосъобразност–правно основание за обработката |

Моля, попълнете таблицата, като отговорите на поставените въпроси.

|  |  |
| --- | --- |
| Въпроси | Отговори |
| На какво основание се извършва обработката? | Съгласие на субекта на данните  Договор, по който субектът на данните е страна, или за предприемане на стъпки по искане на субекта на данните преди сключването на договор  Законово задължение, което се прилага спрямо администратора  Задача от обществен интерес или упражняване на официални правомощия, които са предоставени на администратора |
| Конкретизирайте основанието (напр. ако е законово задължение, посочете къде е предвидено задължението, ако е договор-посочете договора) |  |
|  |  |
| Ако данните не се събират директно от организацията-има ли договорни или законови ограничения в дейностите по обработка, които организацията трябва да спазва? |  |

|  |
| --- |
| Точност |

Моля, попълнете таблицата, като отговорите на поставените въпроси.

|  |  |
| --- | --- |
| Въпроси | Отговори |
| Как е осигурено спазването на изискването данните да бъдат точни и при необходимост да се актуализират? |  |
| Има ли вероятност да се обработват лични данни, които не са точни? |  |

|  |
| --- |
| Свеждане да данните до минимум |

Моля, попълнете таблицата, като отговорите на поставените въпроси.

|  |  |
| --- | --- |
| Въпроси | Отговори |
| Всички лични данни ли са подходящи, свързани със и ограничени до необходимото във връзка с целите, за които се обработват? |  |
| Моля аргументирайте необходимостта и пропорционалността на обработваните данни за постигане на определените цели |  |

|  |
| --- |
| Ограничение на срока |

Моля, попълнете таблицата, като отговорите на поставените въпроси.

|  |  |
| --- | --- |
| Въпроси | Отговори |
| В какъв срок ще се съхраняват личните данни? | Срокът е конкретно определен (посочете срока)……………………..  Срокът на съхранение се определя по следните критерии (посочете критериите) …………………………………………………………….. |
| Как се определя посоченият срок? |  |
| Възможно ли е данните да бъдат обработвани извън установения срок? |  |
| Унищожават ли се данните след изтичане на срока по начин, който не позволява възстановяването им? |  |

|  |
| --- |
| Цялостност и поверителност |

Моля, попълнете таблицата, като отговорите на поставените въпроси.

|  |  |
| --- | --- |
| Въпроси | Отговори |
| Къде се съхраняват личните данни? | На сървър, физически разположен в сграда на организацията  На носител, физически разположен в рамките на ЕС, но извън контрола на организацията  На носител, физически разположен в трета държава  Данните не се съхраняват |
| Контролира ли се достъпът до носителя на данните?  Ако да- по какъв принцип се осигурява достъпът? |  |
| Предоставя ли се достъп от разстояние?  Ако да– от кои държави е възможен достъпът? |  |
| Какви технически и организационни мерки за защита са осигурени? |  |
| Извършва ли се анонимизиране или псевдонимизиране на данните? |  |
| Възможно ли е да бъдат възстановени наличността и достъпът до данните в разумни срокове в случай на физически или технически инцидент? |  |
| Установена ли е процедура/изискване за редовно тестване и оценка на ефективността на осигурените технически и организационни мерки? |  |
| Приложими ли са одобрени кодекси за поведение? |  |
| Извършено ли е сертифициране за защита на данните? |  |

Информиране на субекта на данните

Моля, попълнете таблицата, като отговорите на поставените въпроси.

|  |  |
| --- | --- |
| Въпроси | Отговори |
| Създадени ли са условия за изпълнение на задължението за информирането на субекта на данните за процесите по обработка, извършвани от администратора? |  |
| Съдържанието на предоставената информация отговаря ли на изискванията на чл. 13 от регламента |  |
| Има ли процес, чрез който да се установи каква информация е предоставена на какви лица? |  |

Права на субекта на данните

Моля, попълнете таблицата, като отговорите на поставените въпроси.

|  |  |
| --- | --- |
| Въпроси | Отговори |
| Ясно ли е за лицата по какъв начин може да упражнява правата си като субект на данните? |  |
| Ясно ли е кое право е приложимо по отношение на всеки вид данни? |  |
| Създадени ли са условия за упражняване на правото на преносимост? |  |
| Създадени ли са условия за оттегляне на съгласието, което да се извършва толкова лесно, колкото и оттеглянето? |  |
| Налична ли е възможност за лесна корекция и/или изтриване на всички данни, които се отнасят за определено лице? |  |
| Когато обработката е за изпълнение на задача от обществен интерес или упражняване на официални правомощия, които са предоставени на администратора, както и за защита на легитимните интереси на администратора или на трета страна, има ли ред за преустановяване на обработката след възражение от субекта и за уведомяване за надделяващ над този на субекта на данните интерес? |  |
| Когато обработката е защита на легитимните интереси на администратора или на трета страна, но е установен надделяващ интерес на субекта на данните, осигурена ли е възможност за изтриване на данните на лицето, което е направило такова искане? |  |
| Когато лицето е обект на решение, основаващо се единствено на автоматизирано обработване, включващо профилиране, което поражда правни последствия за субекта на данните или по подобен начин го засяга в значителна степен, може ли да поиска човешка намеса или да оспори решението? |  |
| Създадена ли е възможност за упражняване на правото на ограничаване на обработката? |  |
| Ако субект поиска да упражни правото си на достъп, възможно ли е данните да бъдат извлечени от системата по лесен начин? |  |

Разкриване на лични данни

Моля, попълнете таблицата, като отговорите на поставените въпроси.

|  |  |
| --- | --- |
| Въпроси | Отговори |
|  |  |
| С кого ще бъдат споделени данните, създадени в резултат на процеса? | Обработката се извършва само в рамките на организацията  С обработващ лични данни (моля посочете договора)…………………………………………………………………….  Със съвместен администратор (моля посочете договора)…………………………………………………………………….  С друг администратор, който има собствено основание за обработката (посочете администратора и основанието за предаваното на данните)……………………………………………………………………………. |
| Посочете причината, която налага разкриването. |  |
| Посочете всички видове данни, които се разкриват. |  |
| Включени ли са правила за обработката на личните данни в договорите на всички обработващи? |  |
| Има ли лица, пред които се разкриват данните, които са локализирани в трета страна?  Посочете държавите, в които са локализирани и държавите, в които могат да съхраняват данните |  |
| Ако се извършва предаване в трети държави, спазени ли са правилата за трансфер на данните? |  |

Установяване и оценка на риска

|  |  |  |  |
| --- | --- | --- | --- |
| **Опишете източника на риска и естеството на потенциалното въздействие върху физическите лица.** Включете съответното съответствие и корпоративните рискове, ако е необходимо. | **Вероятност за вреда** | **Тежестта на вредата** | **Общ риск** |
|  | Малко вероятно, възможно или вероятно | Минимална, значима или тежка | Нисък, среден или висок |

Мерки за преодоляване на рисковете

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Определете допълнителни мерки, които можете да предприемете, за да намалите или елиминирате рисковете, идентифицирани като средни или високи рискове в стъпка 5** | | | | |
| **Риск** | **Опции за намаляване или елиминиране на риска** | **Ефект върху риска** | **Остатъчен риск** | **Мярката е одобрена** |
|  |  | Премахнат,  Намален,  Одобрен/приет | Нисък, среден, висок | Да/Не |

Приключване на ОВЗД и актуализация

|  |  |  |
| --- | --- | --- |
| **Предмет** | **Име/дата** | **Бележки** |
| Мерките са одобрени от: |  | Интегриране на дейностите обратно в плана на проекта, с дата и отговорност за изпълнение |
| Остатъчните рискове са одобрени от: |  | Ако приемете остатъчен висок риск, консултирайте се с КЗЛД, преди да продължите напред |
| Предоставени съвети от ДЛЗД: |  | ДЛЗД трябва да даде съвети относно спазването на мерките от стъпка 6 и дали обработката може да продължи |
| Обобщение на съветите на ДЛЗД: | | |
| Препоръките на ДЛЗД, приети или отхвърлени от: |  | Ако бъдат отхвърлени/отменени, трябва да обясните причините си: |
| Коментари: | | |
| Отговори от консултации, разгледани от: |  | Ако решението ви се отклонява от възгледите на отделните хора, трябва да обясните причините за това |
| Коментари: | | |
| Тази ОВЗД ще бъде подложена на преглед от: |  | ДЛЗД трябва също така да преразгледа текущото съответствие с ОВЗД |

1. Виж „Насоки относно оценката на въздействието върху защитата на данни (ОВЗД) и определяне дали съществува вероятност обработването „да породи висок риск“ за целите на Регламент 2016/679“ [↑](#footnote-ref-1)