**Утвърдил:**

 **…………………………..**

 **Управител**

**ПЛАН ЗА ДЕЙСТВИЕ ЗА СПРАВЯНЕ НА РИСКА ПРИ ОБРАБОТКА НА ЛИЧНИ ДАННИ В ......................................................................**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **№** | **Риск** | **Собственик на риска** | **Необходими допълнителни механизми за контрол /за рискове над приемливия/** | **Отговорен за изплънение на Плана за въздействие** | **Срок за изплънение** |
| 1 | Риск целите на обработване на личните данни да не бъдат законни, конкретни и ясно формулирани | Всички служители, които оперират с данни | Да се определят конкретни и ясни цели на обработване на лични данни. Личните данни се събират за конкретни цели | Управител | Веднъж в годината да се прави инвентаризация на целите на обработване на данните |
| 2 | Законност на обработката и забрана за злоупотреба | Всички служители, които оперират с данни | Да се провежда обучение на новопостъпили служители по правилата и политиките за обработка на личните данни. | Управител | Постоянен |
| 3 | Риск от събиране на данни в по-голям обем от нужното (чл.5.1 (в) GDPR) | Всички служители, които оперират с данни | Веднъж на 2 години да се прави инвентаризация на обема на събираните данни по дейности на обработка и да се предприемат дейности за тяхното минимизиране при необходимост. | Управител | веднъж на 2 години |
| 4 | Риск от неточност и неактуалност на данните/чл.5.1 (г) GDPR/ | Всички служители, които оперират с данни | Да се създаде механизъм за актуализиране на данните, получени от първични администратори. Всички служители да се обучат на правилата за актуалзиране на данните. Всеки новопостъпил служител дасе обучи на правилата за актуализиране на данните. | Управител | Създаване на механизъм - до 6 месеца от приемане на плана за въздействие. Еднократно обучение на всички служители, които обработват данните. Обучение на новопостъпили служители |
| 5 | Риск от нарушаване на правото на субекта да бъде информиран (чл. 12, чл.13 и чл.14 GDPR ) | Управител | Разработване и спазване на политики за предоставяне на информация, необходима на субекта на данни, в кратка, прозрачна и разбираема форма | Управител | Възможно най-кратки срокове |
| 6 | Неполучаване на съгласие за обработване, когато е приложимо | Управител | Разработване и спазване на политики за получаване на съгласие и описание на дейностите по обработка с необходимо съгласие. | Управител |   |
| 7 | Рискове свързани с правото на коригиране и на изтриване на данните (чл. 16, чл.17 и чл.19 GDPR ) | Управител | Разработване и спазване на политики за коригиране и изтриване на данните | Управител |   |
| 8 | Нарушаване на правото на на възражение и на ограничаване на обработването (чл. 18, чл.19 и чл.21 GDPR ) | Управител | Разработване и спазване на политики за възражение за обработване и ограничаване на обработването на данните | Управител |   |
| 9 | Нарушаване на поверителността на информацията свързана с личните данни на служителите. |  Управител | Обучение на специалист човешкиресурси по политиките за защита на данните и дейностите по обработка, свързани със служителите. Прилагане на дисциплинарна практика в съответствие с КТ, Правилника за вътрешния трудов ред. Подобряване на контрола за достъп до данни на служителите. | Управител | При въвеждане на политиките и при постъпване на нов служител. |
| Системен администратор; | Системен администратор | Постоянен |
| 10 | Възникване на заплахи за сигурността на информацията вследствие на неприлагане на утвърдените изискванията свързани със сигурността на данните. | Системен администратор | Политика за създаване, обработка и съхранение на ел. документи и обучение на служителите за работа с тази политика | Управител | Създаване на политики и правила за създаване, обработка и съхранение на ел. документи - до 6 месеца. Провеждане на първоначално обучение при въвеждане на политиките. Обучение на новопостъпили служители при постъпване. |
| 11 | Заплахи за сигурността на личните данни, свързани с начините за съхранение в електронна форма в база данни, включително ограничаване на съхранението /чл.5.1 (д) и чл.5.1 (е) GDPR/ | Системен администратор | Ведръж на всеки 5 години да се прави проверка на сроковете за съхранение на отделните типове данни. Да се въведе политика за криптиране на архивираните данни и данните на преносими устройства. Да се извършва поддръжка и валидиране на софтуера за обработкана архивираните данни. Да се въведат политика зи изтриване на чувствителни данни.  | Управител | до 6 месеца |
| 12 | Заплахи свързани с неточности в данните породено от грешки при ръчното въвеждане поради непълната автоматизация на работните процеси | ПолзвателиУправител | Въвеждане на организационни форми за повторна проверка. Автоматизация на различните процеси. Свеждане на обработваните данни до минимум | Управител |  Постоянен |
| 13 | Загуба на информационни активи- лични данни, при възстановяването им от резервирана информация. | Управител | Регулярна проверка на резервираната информация и регистриране на извършената проверк от системния администратор. Създаване на архив на независим сървър/ устройство, което не е включено в мрежата и няма достъп до него | Системен администратор | Всеки месец |
| 14 | Риск от невъзможност за изтриване, заличаване на лични данни при поискване от субекта | Управител | Въвеждане на политики за отговор на искания от субектана данните. Въвеждане на правила и политики за трайно изтривване/ заличаване на данни, за които е възможно | Управител |  Постоянен |
| 15 | Нарушаване на поверителността на част от информацията във функционално звено "човешки ресурси" вследствие на неоторизиран достъп на вътрешен служител. | Управител | Въвеждане на политики за проучване и подбор на персонала преди постъпване наработа. Въвеждане на правила за дисциплинарни наказания в Правилника з вътрешния трудов ред | Управител |  Постоянен |
| 16 | Нарушаване на поверителността на информацията вследствие на несъответстващо на политиката за приемливо използване на информация свързана с лични данни от служители. | Управител | Политика за сигурност при работа с мобилни активи и телекомуникации. Политика за отдалечен достъп. Политика за сигурност на оборудването извън сградата на Дома. Сигурност на оборудването. Създаване на политики с разрешени и забранени дейности по обработка на лични данни | Управител |  Постоянен |
| 17 | Нарушаване на цялостта и поверителността на информация с ЛД вследствие на допускане на злонамерен софтуер в ИС | Системен администратор. |  Политика за сигурност срещу зловредни програми. Политика за сигурност при работа с мобилни активи и телекомуникации. Правила за защита и проверка на маршрутизатор. Проверка на активите за електронна обработка на данни | Системен администратор | Срок за въвеждане на политиките |
| 18 | Нарушаване на цялостта и поверителността на информацията вследствие на проява на небрежност от новоназначен служител или с намерение за вреда | Управител | Проучване на кандидатите за работа за предишни инциденти, свързани с лоялност към предишни работодатели. Обучение на новопостъпили служители по правилата и политиките за обработка на личнитеданни и сигурността на информацията | Управител | Постоянен |
| 19 | Загуба на информация вследствие на кражба или загуба на преносими устройства съхраняващи данни на субекти. | Управител | Политика по автентификация и управление на паролите, Политика за сигурност на оборудването извън работните помещения. Политика за сигурност при идентифициране на инциденти, свързани с ИС.  | Управител |  Постоянен |
| 20 | Риск от загуба на информация и лични данни при извършване на поддръжка и ремонт на сградата, оборудването, системите. | Управител | Изготвяне на клаузи за конфиденциалност към доставчиците и фирмите за поддръжка, определяне на приемливо поведение и изисквания към тях. Извършване на оценка за работата на доставчиците на услуги по поддръжка за качеството на извършената от тях работа веднъж в годината. Преместване на личните данни на хартиен или електронен носител от помещенията в които се извъшва пребоядисване или СМР | Управител | Постоянен |