гр.София,
ул. "Хайдушка гора" 54
+359 890 111 375
office@danaya.bg
www.danaya.bg

ПОЛИТИКА ЗА ОБРАБОТВАНЕ И ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

Съдържание

I. ОБЩА ЧАСТ

Чл. 1. (1) С настоящата политика се уреждат редът и условията за събиране, обработване, актуализация, съхраняване, предоставяне, трансфер и унищожаване на личните данни, както и мерките и средствата за тяхната защита, прилагани от администратора на лични данни Фондация „Даная“.

(2) Настоящата политика се приема с цел да се отговори на изискванията на Регламент (ЕС) 2016/679 (Общ регламент относно защитата на данните) и Закона за защита на личните данни (ЗЗЛД).

(3) Политиката се утвърждава, допълва, изменя и отменя от Ръководството на Фондация „Даная“.

(4) Администраторът предоставя достъп до обработваните от него лични данни на субектите на данни и на трети лица съобразно Регламент (ЕС) 2016/679 на ЕС и ЗЗЛД.

гр.София,
ул. "Хайдушка гора" 54
+359 890 111 375
office@danaya.bg
www.danaya.bg

II. ЦЕЛИ И ОБХВАТ НА ПОЛИТИКАТА

Чл. 2. Настоящата Политика има за цел да регламентира:

а) механизмите за събиране, обработване, актуализация, съхраняване, предоставяне, трансфер и унищожаване на личните данни;

б) задълженията на Администратора, лицата, обработващи лични данни, отговорното лице по защита на данните и тяхната отговорност при неизпълнение на тези задължения.

III. ЗАКОНОСЪОБРАЗНОСТ НА ОБРАБОТВАНЕТО. СПЕЦИФИКИ

Чл. 3. (1) Личните данни в организацията на Администратора подлежат на обработване в съответствие с принципите за законосъобразност, добросъвестност и прозрачност, установени съгласно чл. 5 от Регламент (ЕС) 2016/679.

(2) Лични данни ще бъдат обработвани само в случаите, когато е налично поне едно от посочените в чл. 6 на Регламент (ЕС) 2016/679 основания за обработване.

(3) При прилагане на настоящата политика се отчита специфичният обществено-полезен профил на Фондация „Даная“ - подкрепа на деца-пациенти, деца-ученици и техните родители, включително чрез юридическа, психологическа, информационна, консултативна, социална, образователна и организационна подкрепа.

(4) При всички дейности, свързани с деца и със здравни данни, Фондацията прилага повишени стандарти за поверителност, минимизиране на данните, контрол на достъпа, документиране на действията и ограничаване на сроковете за съхранение.

IV. ИЗПОЛЗВАНИ ПОНЯТИЯ

Администратор – под „администратор“ в настоящата политика се има предвид Фондация „Даная“, гр. София, ж.к. „Младост 2“, блок 282Б, вх. 1, ет. 1, магазин 1, телефон: +359 890 111 375, електронна поща: office@danaya.bg, интернет страница: www.danaya.bg.

Служители и сътрудници – под „служители и сътрудници“ в настоящата политика се имат предвид всички работещи по трудово или гражданско правоотношение, доброволци, външни консултанти, членове на консултативни органи и други лица, които трайно съдействат на Фондация „Даная“.

Ръководство – под „ръководство“ в настоящата политика се имат предвид Ръководството на Фондация „Даная“ и лицата, които представляват или управляват дейността на Фондацията.

Субект на лични данни – всички физически лица, чиито лични данни се обработват от Фондация „Даная“.

Носители на лични данни – всички физически и виртуални средства, които способстват за съхранението и обработването на лични данни – компютри и софтуерни приложения, преносими устройства, хартиени досиета, заключени шкафове, корпоративна електронна поща, Google Drive, уеб поща, платформи, онлайн форми, регистри, архиви и други информационни ресурси.

гр.София,
ул. "Хайдушка гора" 54
+359 890 111 375
office@danaya.bg
www.danaya.bg

V. ОТГОВОРНО ЛИЦЕ ПО ЗАЩИТА НА ДАННИТЕ

Чл. 4. Администраторът определя отговорно лице по защита на данните (ОЛЗД), което:

а) информира и съветва Администратора и служителите, които извършват обработване, за техните задължения по силата на действащото законодателство;

б) наблюдава спазването на настоящата политика и изискванията на законодателството за защита на личните данни, включително възлагането на отговорности, повишаването на осведомеността и обучението на персонала, участващ в операциите по обработване, и съответните проверки;

в) при поискване предоставя съвети по отношение на оценката на въздействието върху защитата на данните и наблюдава извършването на оценката;

г) сътрудничи си с надзорния орган и действа като точка за контакт за надзорния орган по въпроси, свързани с обработването, включително предварителната консултация, посочена в член 36, и по целесъобразност да се консултира по всякакви други въпроси.

VI. РЕГИСТЪР НА ДЕЙНОСТИТЕ ПО ОБРАБОТВАНЕ НА АДМИНИСТРАТОРА

Чл. 5. Дейностите по обработване на лични данни, извършвани в организацията на Администратора, се описват в „Регистър на дейностите по обработване“, съгласно чл. 30, параграф 1 от Регламент (ЕС) 2016/679.

Чл. 6. (1) Регистърът на дейностите по обработване на Администратора се съставя от Администратора и се поддържа в актуален вид от Отговорното лице по защита на данните, както и се предоставя на надзорния орган при проверка.

(2) „Регистърът на дейностите по обработване на администратора“ е част от системата за отчетност на Фондацията и се поддържа във вида му, посочен в Приложение № 9 към настоящата политика, заедно с относимите балансиращи тестове.

VII. ОСИГУРЯВАНЕ НА ПРОЗРАЧНОСТ ПРИ ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ

Чл. 7. В рамките на организацията на Администратора се гарантира съответствие с изискванията за прозрачност при обработването на лични данни.

Чл. 8. Администраторът, съгласно изискванията на ОРЗД, предоставя на субектите на данни законово изискваната информация във вид на „Уведомление (политика) за поверително третиране на личните данни“.

Чл. 9. Администраторът поставя тези съобщения на всички „точки за контакт“ със субектите на данни, като например интернет страница, деловодство и други, така че да осигури лесен достъп до тях.

Чл. 10. (1) Администраторът, с помощта на ОЛЗД, е длъжен да контролира и поддържа механизмите за информиране, които да дават възможност на субектите на лични данни да се запознаят със съдържанието на съответното уведомление преди да събира техните данни.

гр.София,
ул. "Хайдушка гора" 54
+359 890 111 375
office@danaya.bg
www.danaya.bg

(2) „Уведомлението за поверителност“ трябва да съдържа информацията от образците, посочени като Приложения № 7.1 - 7.5 към настоящата политика.

Чл. 11. Администраторът предоставя при събиране на лични данни от субекта на данни следната информация:

1. данните, които идентифицират Фондация „Даная“ и координатите за връзка с нея;
2. данните за контакт с Отговорното лице по защита на данните на Фондация „Даная“;
3. целите на обработването, за което личните данни са предназначени;
4. правното основание за обработването на личните данни;
5. категориите лични данни, които се обработват;
6. получателите или категориите получатели на личните данни (ако има такива);
7. срока, за който ще се съхраняват личните данни от Администратора, а ако това е невъзможно - критериите, използвани за определяне на този срок;
8. указание към субекта на лични данни за правата му да изиска от Администратора достъп до данните, коригиране или изтриване на неговите лични данни, както и правата му на ограничаване на обработването, на възражение срещу обработването, както и на преносимост на данните;
9. когато правното основание за обработването е съгласие, Администраторът уведомява субекта на данни за съществуването на право на оттегляне на съгласието по всяко време, както и за законосъобразността на обработването до момента на оттеглянето;
10. правото на жалба до надзорен орган;
11. наличието на автоматизирано вземане на решения, включително профилиране, както и предвидените последствия от това обработване за субекта на данните;
12. когато правното основание не е съгласие на субекта, а е задължително или договорно изискване, или изискване, необходимо за сключването на договор, Администраторът уведомява субекта на данни за това, а също и дали е длъжен да предостави личните данни и евентуалните последствия, ако тези данни не бъдат предоставени.

Чл. 12. Когато лични данни са получени от източник, различен от субекта на данните, Администраторът предоставя следната информация:

1. данните, които идентифицират Фондация „Даная“ и координатите за връзка с нея;
2. данните за контакт с Отговорното лице по защита на данните на Фондация „Даная“;
3. целите на обработването;
4. правното основание за обработването;

гр.София,
ул. "Хайдушка гора" 54
+359 890 111 375
office@danaya.bg
www.danaya.bg

5. законните интереси, преследвани от Администратора или от трета страна, ако се обработват на това основание;
6. категориите лични данни, които се обработват;
7. потенциалните получатели / категориите получатели на личните данни;
8. намерението на Администратора да извърши предаване на данните на трета държава извън ЕС или на международна организация, съответните гаранции за защита на данните и средствата за получаване на копие от тях или на информация къде са налични;
9. указание към субекта на лични данни за правата му да изиска достъп до данните, коригиране или изтриване на неговите лични данни, както и правата му на ограничаване на обработването, на възражение срещу обработването и на преносимост на данните;
10. когато правното основание за обработването е съгласие, Администраторът уведомява субекта на данни за съществуването на право на оттегляне на съгласието по всяко време, както и за законосъобразността на обработването до момента на оттегляне;
11. правото на жалба до надзорен орган;
12. източника на личните данни и дали данните са от публично достъпен източник;
13. наличието на автоматизирано вземане на решения, включително профилиране, както и предвидените последствия от това обработване за субекта на данните;
14. срокът, за който ще се съхраняват личните данни, а ако това е невъзможно - критериите, използвани за определяне на този срок.

Чл. 13. При предоставянето на данните за осигуряване на прозрачност, Фондация „Даная“ спазва следните изисквания на ОРЗД:

1. при събирането на лични данни от субекта на данни, Администраторът предоставя на субекта посочената информация в момента на получаване на информацията;
2. при събирането на лични данни от източник, РАЗЛИЧЕН ОТ субекта на данните, Администраторът предоставя на субекта посочената информация в срок от един месец от получаване на личните данни в съответствие със специфичните обстоятелства на обработването;
3. в случаите, когато данните се използват за комуникация със субекта на данни, Фондация „Даная“ съобщава информацията най-късно при осъществяване на първия контакт с него;
4. в случаите, когато личните данни се разкриват на друг получател, Фондация „Даная“ съобщава информацията най-късно при разкриването на личните данни за първи път;

гр.София,
ул. "Хайдушка гора" 54
+359 890 111 375
office@danaya.bg
www.danaya.bg

5. Администраторът НЕ предоставя тази информация, ако субектът на данните вече разполага с нея;
6. Администраторът НЕ предоставя тази информация, в случай че предоставянето се окаже невъзможно или би довело до прекомерно усилие за организацията на Администратора;
7. Администраторът няма задължение да предостави тази информация, в случай че получаването или разкриването на лични данни е изрично регламентирано от националното законодателство;
8. Администраторът предоставя на субекта на данните всяка допълнителна информация, която е необходима за осигуряване на добросъвестно и прозрачно обработване.

VIII. УПРАВЛЕНИЕ НА ИСКАНИЯТА ОТ СУБЕКТИТЕ НА ЛИЧНИ ДАННИ

Чл. 14. (1) Отговорното лице по защита на данните отговаря за обработването на всички искания на субекта на данни, които са резултат от упражняване на правата, дадени им съгласно Общия регламент относно защитата на данните и ЗЗЛД.

(2) Подробният ред за приемане, регистриране, разглеждане, документиране и отговор на исканията за упражняване на права е уреден в Политика за управление на искания от субекти на лични данни - Приложение № 3 към настоящата политика.

Чл. 15. (1) При отправянето на искане субектът на данни указва конкретния вид искане в свободна форма или в образеца на формата, предоставена от Администратора и публикувана на интернет страницата му.

(2) Образецът на форма за „Искане от субекта на данни“ е посочен като Приложение № 13 към настоящата политика.

Чл. 16. При отправяне на искане се спазват следните правила:

1. Субектът на данните може да поиска всички негови лични данни, съхранявани от Администратора без да указва конкретен вид;
2. Субектът на данните предоставя на Администратора данни за самоличността си, които да го идентифицират сигурно и еднозначно;
3. Администраторът задължително проверява идентификационните данни, за да се увери, че искането е подадено от субекта, който данните идентифицират;
4. Администраторът документира датата на получаване на искането чрез вписването му във входящата поща;
5. След като искането бъде получено, то незабавно се препраща до Отговорното лице по защита на данните, което ръководи процеса по обработване на искането и изпращането на отговор на субекта на данните.

Чл. 17. Обработването на искането се извършва по следния ред:

гр.София,
ул. "Хайдушка гора" 54
+359 890 111 375
office@danaya.bg
www.danaya.bg

1. Отговорното лице по защита на данните вписва в Регистъра на исканията от субекти на данните датата, идентифициращата информация и всички други важни за разглеждане на искането данни;
2. Идентифицирането (търсенето) на личните данни се извършва във всички хранилища на данни и всички съответни системи за архивиране, включително всички архивирани файлове (компютъризирани или хартиени архиви) и всички папки на електронната поща и техните архиви;
3. Когато искането е за достъп до информация, при предаването на копие от информацията Отговорното лице по защита на данните извършва обработване на данните с цел отстраняване на евентуална идентификационна информация за трети лица;
4. Администраторът предоставя исканата информация и отговаря на исканията на субекта на данните в рамките най-късно на един месец от датата на получаване на искането за достъп. При необходимост този срок може да бъде удължен с още два месеца, като се взема предвид сложността. Администраторът информира субекта на данните за всяко такова удължаване в срок от един месец от получаване на искането, като посочва и причините за забавянето;
5. Отговорното лице за защита на данните вписва в Регистъра на исканията данни за подадения към субекта отговор на искането за достъп. Отговорното лице по защита на данните поддържа „Регистър на исканията от субекти на данните“ съгласно Приложение № 10.1 към настоящата политика.

Чл. 18. В случай на искане от субекта на данни за получаване на достъп до данните, освен че осигурява достъп до данните (например чрез предоставяне на тяхно копие), Администраторът изпраща на субекта и следната информация:

1. целите на обработването;
2. съответните категории лични данни;
3. получателите или категориите получатели на личните данни (ако има такива);
4. информация относно намерението на Администратора да предаде данните на трета държава или на международна организация, както и наличието на гаранции за защита на данните;
5. срока, за който Администраторът ще съхранява личните данни, а ако това е невъзможно - критериите, използвани за определяне на този срок;
6. правата му да се изиска от Администратора коригиране или изтриване на неговите лични данни, както и правата му на ограничаване на обработването, на възражение срещу обработването, както и на преносимост на данните;
7. правото на жалба до надзорен орган;
8. когато личните данни не се събират от субекта на данните - всякаква налична информация за техния източник;

гр.София,
ул. "Хайдушка гора" 54
+359 890 111 375
office@danaya.bg
www.danaya.bg

9. наличие на автоматизирано вземане на решения, включително профилиране, както и предвидените последствия от това обработване за субекта на данните.

Чл. 19. Когато исканията на субект на данни са явно неоснователни или прекомерни, по-специално поради своята повторяемост, Отговорното лице по защита на данните може:

1. да предложи на ръководството на Администратора да наложи разумна такса, като взема предвид административните разходи за предоставяне на информацията или комуникацията или предприемането на исканите действия;
2. да предложи на ръководството на Администратора да откаже да предприеме действия по искането.

Чл. 20. При искане на субекта на данни за коригиране, изтриване, ограничаване или при възражение по отношение на обработваните лични данни Отговорното лице по защита на данните преценява всяко от тези искания (извън искането за достъп до данни) с оглед основателността на правото на субекта и наличието на други законови изисквания за неговото удовлетворяване.

Чл. 21. След като се установи основателността на съответното искане или възражение Администраторът извършва следните действия:

1. премахва личните данни от системите и прекратява операциите по обработването им, без ненужно забавяне, ако искането за изтриване е подадено от субекта на данните;
2. съобщава на субекта на данни за всяко извършено коригиране, изтриване или ограничаване на обработването на всеки получател, на когото личните данни са били разкрити;
3. информира субекта на данните относно получателите на данни, ако субектът на данните поиска това, и документира това съобщение.

IX. ПОЛУЧАВАНЕ НА СЪГЛАСИЕ ЗА ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ

Чл. 22. (1) Администраторът на данни в своята дейност по обработване на лични данни се ръководи от законовото положение, че съгласието на субекта на данните е едно от правните основания за обработването на лични данни и попада в обхвата на настоящата политика.

(2) Администраторът използва съгласието като основание за обработване на данни, когато данните не се обработват на друго правно основание.

(3) Когато обработването се основава на съгласие, Фондацията прилага отделими, ясни и доказуеми механизми за получаване и оттегляне на съгласие, съобразно конкретната категория субекти и съответното уведомление за поверителност.

Чл. 23. Администраторът предоставя ясна информация чрез Уведомление за поверително третиране на личните данни, за да гарантира, че съгласието е информирано и че субектът на данни е информиран за правата си във връзка с обработването на личните му данни.

гр.София,
ул. "Хайдушка гора" 54
+359 890 111 375
office@danaya.bg
www.danaya.bg

Чл. 24. Съгласието на субекта на данни се взема във формата на писмен документ с цел лесно да се установи, че:

а) е налице съгласие от субекта на данните за обработването на неговите лични данни, респ. че е дадено изрично съгласие за чувствителни лични данни;

б) субектът на данните е информиран за правото си да оттегли съгласието, преди да даде съгласието си;

в) субектът на данните е информиран, че оттеглянето на съгласието не засяга законосъобразността на обработването, основано на дадено съгласие преди неговото оттегляне.

Чл. 25. Когато обработването на лични данни е свързано с дете на възраст под 14 години, Администраторът иска съгласие от лицето, което носи родителска отговорност за детето.

Чл. 26. Субектът на данни има правото да оттегли съгласието си по всяко време чрез недвусмислено волеизявление.

Чл. 27. Оттеглянето на съгласието не засяга законосъобразността на обработването, основано на дадено съгласие преди неговото оттегляне. Преди да даде съгласие, субектът на данни бива информиран за това условие.

Чл. 28. Доколкото съгласието обхваща всички дейности по обработване на данните, извършвани с една и съща цел или цели, оттеглянето на съгласието действа относно дейностите за обработване на данни, извършвани за същата цел или цели.

Чл. 29. Даване, документиране и оттегляне на съгласие се извършва чрез подходящи писмени, електронни или други доказуеми механизми, определени от Администратора според конкретната дейност по обработване, категорията субекти на данни и вида на обработваните лични данни. Администраторът поддържа доказателства за даденото съгласие, неговия обхват, датата и начина на получаване, както и за евентуалното му оттегляне.

X. УВЕДОМЯВАНЕ ЗА НАРУШЕНИЕ НА СИГУРНОСТТА НА ЛИЧНИТЕ ДАННИ

Чл. 30. (1) В настоящата политика са изложени общите правила, които определят действията в случай на нарушение на сигурността на личните данни. Подробният ред за идентифициране, регистриране, ескалация, оценка и овладяване на инциденти е уреден в Политиката за реагиране на инциденти (Приложение № 4). При оценка на тежестта на нарушение се прилага Методиката за оценка на тежестта на пробиви в сигурността на личните данни (Приложение № 11), а нарушенията се вписват в Регистъра за нарушенията на сигурността (Приложение № 10.2).

(2) При установяване на такива нарушения, служителите, които ги установят, незабавно уведомяват ръководството на Администратора или Отговорното лице по защита на данните (ОЛЗД).

(3) Администраторът, с помощта на ОЛЗД, извършва оценка на въздействието на нарушението.

гр.София,
ул. "Хайдушка гора" 54
+359 890 111 375
office@danaya.bg
www.danaya.bg

Чл. 31. (1) Ако установи, че съществува риск за правата и свободите на субектите на данни, Администраторът чрез ОЛЗД уведомява надзорния орган за нарушението на сигурността на личните данни без ненужно забавяне и не по-късно от 72 часа след като е узнал за него.

(2) В случай че уведомлението не е направено в рамките на 72 часа, Отговорното лице по защита на данните уведомява надзорния орган при първа възможност, като към уведомлението в допълнение излага причините за забавянето.

Чл. 32. (1) Уведомлението до надзорния орган трябва да съдържа следната информация:

а) описание на естеството на нарушението на сигурността на личните данни;

б) категориите лични данни, засегнати от нарушението;

в) категориите и приблизителния брой на засегнатите субекти на данни;

г) приблизителното количество на засегнатите записи на лични данни;

д) имената и контактните данни на Отговорното лице по защита на данните;

е) описание на последиците от нарушението на сигурността;

ж) предприетите или предложените от Администратора мерки за справяне с нарушението.

(2) Когато и доколкото не е възможно цялата необходима информация да се подаде едновременно, тя се подава поетапно без по-нататъшно ненужно забавяне.

(3) Уведомлението до надзорния орган се изпраща съобразно изискваната от надзорния орган форма на комуникация и е съгласно образеца на уведомление, съдържащ се в Политиката за реагиране на инциденти - Приложение № 4 към настоящата политика.

(4) Администраторът документира информацията относно потвърждението от страна на надзорния орган за получаването на уведомлението.

Чл. 33. (1) Когато има вероятност нарушението на сигурността на личните данни да породи висок риск за правата и свободите на субекти на данните, Администраторът, без ненужно забавяне, съобщава на засегнатите субекти на данните за нарушението.

(2) Съобщението до субектите на данни, които са засегнати от нарушението на данните, съдържа същата информация, която се изпраща и до надзорния орган.

(3) Ако нарушението засяга голям брой субекти на данни и записи на лични данни, Администраторът взема решение, основано на оценка на количеството усилия, необходими за уведомяване поотделно на всеки субект на данни и на това дали по този начин би била възпрепятствана способността му да изпрати навреме нужните съобщения.

(4) Когато оценката по ал. 3 покаже, че съобщаването до голям брой субекти би довело до непропорционални усилия, Администраторът прави публично съобщение или взема друга подобна мярка, с която да гарантира, че субектите на данни ще бъдат в еднаква степен ефективно информирани.

гр.София,
ул. "Хайдушка гора" 54
+359 890 111 375
office@danaya.bg
www.danaya.bg

Чл. 34. (1) Администраторът документира в „Регистър на нарушенията на сигурността“ всички нарушения на сигурността на личните данни, като посочва отнасящите се до тях факти, последиците и предприетите мерки за смекчаване на тяхното въздействие.

(2) Регистърът на нарушенията се поддържа от Отговорното лице по защита на данните съгласно образец Приложение № 10.2. към настоящата политика.

XI. ОЦЕНКА НА РИСКА И ОЦЕНКА НА ВЪЗДЕЙСТВИЕТО ВЪРХУ ЗАЩИТАТА НА ДАННИТЕ

Чл. 35. При планирането на всяка дейност, която предвижда обработването на лични данни, Администраторът извършва оценка на риска и ако е необходимо, оценка на въздействието върху защитата на данните (ОВЗД), като взема предвид вида на личните данни и начините за обработването им.

Чл. 36. Служителите, ръководещи отделните процеси по обработване на личните данни, са отговорни за своевременното известяване на Отговорното лице по защита на данните за наличието на нови дейности по обработване.

Чл. 37. Администраторът извършва оценка на риска и ОВЗД с цел определяне на адекватно ниво на технически и организационни мерки за защита на личните данни, което отговаря на обработваните от него лични данни и въздействието при нарушаване на защитата им.

Чл. 38. Администраторът оценява риска, като отчита вероятността за настъпване на съответното нарушение на сигурността на данните и величината на потенциалните неблагоприятни последици за субектите на данни.

Чл. 39. Оценката на риска и оценката на въздействието се извършват на основата на избрана от Администратора и съгласувана с ОЛЗД Методика за оценка на риска и оценка на въздействието, която е неразделна част от настоящата политика като Приложение № 15.

Чл. 40. (1) Оценка на въздействието върху защитата на данните се извършва задължително от Фондация „Даная“, когато с оглед естеството, обхвата, контекста и целите на обработването съществува вероятност то да породи висок риск за правата и свободите на физическите лица.

(2) Оценка на въздействието се извършва задължително и в случаите по чл. 35, пар. 3 от ОРЗД, включително когато:

1. се извършва систематична и подробна оценка на лични аспекти относно физически лица, основана на автоматизирано обработване, включително профилиране, която служи като основание за решения, пораждащи правни последици за лицето или по подобен начин сериозно го засягат;
2. се извършва мащабно обработване на специални категории лични данни по чл. 9 от ОРЗД или на лични данни, свързани с присъди и нарушения по чл. 10 от ОРЗД или се извършва систематично мащабно наблюдение на публично достъпна зона.

(3) При дейности на Фондацията, свързани с деца, пациенти, родители/законни представители, лица в уязвимо положение, здравни, социални или други чувствителни обстоятелства, както и при нова дейност, съществена промяна на съществуваща дейност,

гр.София,
ул. "Хайдушка гора" 54
+359 890 111 375
office@danaya.bg
www.danaya.bg

разширяване на обработването или наличие на обстоятелства, които могат да повишат риска за правата и свободите на субектите на данни, Фондацията извършва предварителна преценка съгласно Методиката за оценка на риска и оценка на въздействието, на спецификата на конкретното обработване и оценката на риска.

(4) Когато съществува съмнение дали конкретна дейност по обработване поражда вероятност от висок риск, както и при наличие на критерии за висок риск или когато в резултат на предварителната преценка се установи вероятност от висок риск, ОВЗД се извършва преди започване, разширяване или съществена промяна на обработването.

XII. ПРАВИЛА ЗА ФИЗИЧЕСКИ ДОСТЪП ДО ПОМЕЩЕНИЯТА И НОСИТЕЛИТЕ С ЛИЧНИ ДАННИ

Чл. 41. (1) Достъпът до сградата на Администратора е ограничен с физически контрол на входа, с цел недопускане на неоторизирани лица.

(2) В извънработно време достъпът до сградата на администратора е ограничен.

(3) За отделни помещения, офиси, архиви или места за съхранение на носители с лични данни Фондацията има право да въведе специфични правила за достъп и контрол, съобразно характера на данните, риска и организацията на работните процеси.

(4) Фондацията използва видеонаблюдение като мярка за сигурност, контрол на достъпа и защита на помещенията, лицата, документите, архивите, техническите средства и имуществото. Видеонаблюдението се извършва при условията и по реда, определени в Политиката за видеонаблюдение — Приложение № 8 към настоящата политика.

Чл. 42. (1) Самостоятелният достъп до помещенията и местата, където се съхраняват носители с лични данни е ограничен само до служителите, които са необходими за осъществяване на работните процеси в организацията на Администратора.

(2) Всяко помещение, в което се съхраняват носители със запис на лични данни, разполага с възможности за заключване и самостоятелният достъп се контролира.

Чл. 43. Като се съобразява с разходите за прилагане и естеството, обхватът, контекстът и целите на обработването, Администраторът ограничава достъпа до всеки носител на лични данни както следва:

а) за компютъризирани носители - с поставяне на парола за достъп на операционната система, на съответния компютър, парола за достъп до съответните софтуерни приложения и разпределение, и контролиране на правата за мрежов достъп;

б) за хартиени носители - със съхраняването в заключени шкафове или сейфове.

Чл. 44. (1) Администраторът определя кои длъжности от работещите за Фондацията имат право на самостоятелен достъп до помещенията с носителите на лични данни.

(2) Под „самостоятелен достъп“ се разбира правото на лицата, заемащи съответните длъжности, да притежават ключове от изброените помещения и да ги достъпват без друг оправомощен служител и без допълнително разрешение от Ръководството на Фондация „Даная“.

гр.София,
ул. "Хайдушка гора" 54
+359 890 111 375
office@danaya.bg
www.danaya.bg

(3) За всички останали лица, които нямат такива права, самостоятелният достъп, без присъствието на оправомощен служител, е забранен.

(4) В дейността си по обработване и защита на личните данни Администраторът прилага „Политика за техническите и организационни мерки за защита на личните данни“ - Приложение № 2 към настоящата политика, която е задължителна за всички негови служители, както и за служителите на договорните партньори на Администратора на лични данни, които имат валидно правно основание за обработване на лични данни и се нуждаят от достъп за изпълнение на договорните си задължения.

XIII. ПРАВИЛА ЗА РЕДА И НАЧИНИТЕ ЗА ЗАЩИТА НА ЕЛЕКТРОННИТЕ ИНФОРМАЦИОННИ НОСИТЕЛИ

Чл. 45. (1) Всички електронни носители на лични данни се защитават с парола за достъп.

(2) Паролите за достъп до съответната операционна система на компютъра или софтуерно приложение за обработване на лични данни трябва да отговарят на определени минимални изисквания, които са конкретизирани в „Политиката за информационна сигурност“, която е Приложение № 5 към настоящата политика.

(3) При напускане на служител или временно заместване на служител, който е имал достъп до съответен компютър или софтуерно приложение със записи на лични данни, паролата се сменя, като новата отговаря на посочените в ал. 2 изисквания.

(4) Всички компютърни работни станции да бъдат настроени с автоматично заключване на достъпа до операционната система в от 5 до 10-минутен интервал (Screen Saver) при липса на работна активност.

Чл. 46. В организацията на Администратора задължително се използват антивирусен софтуер и защитни стени.

Чл. 47. В организацията на Администратора има утвърдени правила за начините на достъп и правата за достъп на мрежовите потребители, както и за сигурността на използваните мобилни устройства.

Чл. 48. Администраторът изготвя, поддържа и прилага „График за създаване на резервни копия (бекъп)“, който е част от Политиката за информационна сигурност, прилагана от Фондацията.

XIV. ПРАВИЛА ЗА УНИЩОЖАВАНЕ НА НОСИТЕЛИ НА ЛИЧНИ ДАННИ

Чл. 49. Най-малко веднъж годишно, Отговорното лице по защита на данните, подпомогнато от Ръководството, прави оценка на подлежащите на унищожаване информационни носители с лични данни – хартиени или електронни, при съобразяване с Политиката за съхраняване и унищожаване на лични данни - Приложение № 6 към настоящата политика и с Графика за съхранение и унищожаване, съдържащ се в Приложение № 6.

Чл. 50. (1) Личните данни с изтекъл срок на съхранение се унищожават от назначена от Ръководството на фондацията тричленна комисия, която задължително включва Отговорното лице по защита на данните.

гр.София,
ул. "Хайдушка гора" 54
+359 890 111 375
office@danaya.bg
www.danaya.bg

(2) Комисията съставя протокол за унищожените носители на лични данни, който включва:

- Вида на унищожените носители;
- Вида и броя записи на лични данни (доколкото това е възможно);
- Броя на унищожените носители, съответните им идентификационни номера (ако имат такива);
- Начините на унищожаване.

Чл. 51. (1) Унищожаване на информацията върху вече неизползвани (бракувани) електронни носители се осъществява от комисията по чл. 50.

(2) При замяна поради технически или организационни причини на записващи носители (компютърни харддискове или други записващи лични данни елементи), комисията се уверява, че информацията е сигурно изтрита или самият носител е унищожен невъзвратимо, така че информацията не може да се извлече.

XV. ОБУЧЕНИЕ

Чл. 52. (1) Администраторът, след консултация с Отговорното лице по защита на данните, възлага на служителите задължения по защита на данните във връзка с настоящата политика за обработване на личните данни.

(2) Отговорното лице по защита на данните запознава служителите относно значението на защитата на данните в изпълнението на преките им задължения.

(3) Служителите получават конкретно обучение за обработване на лични данни, свързани с техните постоянни трудови задължения и отговорности и в съответствие с настоящата политика.

(4) Служителите получават обучение относно процедурите при постъпили за разглеждане искания и възражения от субекти на данните, както и с необходимите действия при нарушаване на сигурността на личните данни, съгласно настоящата политика.

(5) Отговорното лице по защита на данните трябва да се увери, че всички служители, които имат текущи задължения, свързани с лични данни и операции по обработване, както и тези с редовен достъп до лични данни, показват информираност относно изискванията за защита на личните данни.

Чл. 53. Всеки новопостъпил служител, чиято длъжностна характеристика е свързана с обработването на лични данни, подлежи на обучение при назначаване, което задължително включва запознаване с настоящата политика.

Чл. 54. (1) В организацията на Администратора се прави въвеждащо и текущо обучение по защита на личните данни в съответствие с изискванията за поддържане на добро ниво на компетентност.

(2) Веднъж на две години, Администраторът с помощта на ОЛЗД организира опресняващо обучение на служителите, което включва и запознаване с евентуални нови изисквания относно защитата на личните данни.

гр.София,
ул. "Хайдушка гора" 54
+359 890 111 375
office@danaya.bg
www.danaya.bg

Чл. 55. Всяко проведено обучение се документира.

XVI. РЕГЛАМЕНТИРАНЕ НА ВЗАИМООТНОШЕНИЯТА С КОНТРАГЕНТИ

Чл. 56. (1) Администраторът взема мерки за защита на личните данни в процеса на подготовка, сключване и изпълнение на договорни отношения с трети страни (контрагенти, донори, дарители и партньори).

(2) Администраторът сключва писмено споразумение с контрагента по договора и изисква от него да третира личните данни, които ще му станат известни в процеса на изпълнение на договора, като поверителни и да не ги разкрива, освен на служителите си и обработващи подизпълнители и само доколкото това е необходимо за изпълнение на дейностите по договора.

Чл. 57. В случаите, когато договорът е със страна, която се явява обработващ, по смисъла на Общия регламент относно защитата на данните, Администраторът изисква от контрагента да осигури подходящи мерки за сигурност на личните данни, които ще обработва и в споразумението се предвиждат най-малко следните гаранции:

- Задължава обработващия да третира всички лични данни, предадени от Администратора или възникнали по време на обработването, като поверителни, като не ги разкрива, освен на служителите си и обработващи подизпълнители и само доколкото това е необходимо за изпълнение на дейностите по договора;
- Забранява на обработващия да използва от своя страна подизпълнители за обработването на личните данни без изрично писмено разрешение от Администратора;
- В случаите, когато на обработващия бъде разрешено да превъзложи обработването на лични данни на подизпълнител, обработващият от първо ниво трябва да забрани на подизпълнителя от второ ниво (и по-нататък по веригата) да превъзлага дейността по обработка на данни на подизпълнители без писменото разрешение от Администратора;
- Договорите с подизпълнители от второ ниво се одобряват, само ако изискват от тях да спазват най-малко същите разпоредби за сигурност и другите изисквания, които се отнасят и до основната организация обработващ;
- При прекратяването на договор с обработващия или негови подизпълнители, съответните лични данни трябва да бъдат унищожени или върнати на Администратора по веригата от подизпълнители.

Чл. 58. Когато контрагентът действа като обработващ лични данни, се прилага Споразумение между администратор и обработващ за обработване на лични данни (Приложение № 12.1.). Когато страните действат като самостоятелни администратори, се прилага Споразумение между самостоятелни администратори (Приложение № 12.2).

гр.София,
ул. "Хайдушка гора" 54
+359 890 111 375
office@danaya.bg
www.danaya.bg

XVII. ТРАНСФЕР НА ДАННИ

Чл. 59. (1) Предаването на лични данни от Европейския съюз/Европейското икономическо пространство към държава извън ЕС/ЕИП („трета държава“) или към международна организация се допуска само при спазване на изискванията на Глава V от ОРЗД и при осигуряване на ниво на защита на личните данни, което по същество е равностойно на гарантираното в рамките на ЕС/ЕИП. Трета държава е всяка държава, която не е член на Европейския съюз или на Европейското икономическо пространство, включващо Лихтенщайн, Норвегия и Исландия.

(2) Предаването на лични данни към трета държава или международна организация се извършва само когато е налице приложим механизъм за трансфер съгласно Глава V от ОРЗД, включително решение за адекватност, подходящи гаранции като стандартни договорни клаузи или задължителни фирмени правила, или приложима дерогация за конкретна ситуация. При всяко предаване на лични данни извън ЕС/ЕИП Фондацията извършва предварителна проверка на получателя, държавата на получаване, целта и обхвата на предаването, категориите данни, приложимия механизъм за трансфер и необходимостта от допълнителни технически, организационни или договорни мерки.

(3) Фондация „Даная“ може да предава лични данни извън ЕС и ЕИП, когато това е необходимо за изпълнение на нейната дейност, включително при съдействие за лечение на деца-пациенти в чужбина, комуникация с болници, медицински специалисти, институции, партньорски организации, доставчици на услуги или други получатели извън ЕС/ЕИП. Такива трансфери могат да включват данни на деца, родители/законни представители, данни за контакт, документи за представителство, медицински документи, епикризи, становища, резултати от изследвания, информация относно лечение, социална или семейна ситуация и друга документация, необходима за конкретния случай.

(4) Преди извършване на трансфер към трета държава Фондацията проверява дали за съответната държава, територия, сектор или международна организация има действащо решение за адекватност на Европейската комисия, като използва официалната страница на Европейската комисия относно решенията за адекватност. Такива решения съществуват например за Израел, Обединеното кралство, Швейцария и др.

(5) Когато трансферът е единичен, конкретен, неповтарящ се и свързан с индивидуален случай на дете-пациент, включително при спешност, необходимост от бърза медицинска преценка, оферта за лечение, прием в болница или защита на жизненоважни интереси, Фондацията може да прецени приложимостта на изключенията по чл. 49 от ОРЗД. Такива изключения могат да бъдат използвани само при конкретна преценка и не следва да служат като основание за регулярни, масови или системни трансфери. В зависимост от случая приложими могат да бъдат например изрично съгласие на субекта на данните/законния представител след информиране за възможните рискове, необходимост от трансфер за защита на жизненоважни интереси на детето-пациент, когато лицето не е в състояние да даде съгласие, или необходимост от трансфер за установяване, упражняване или защита на правни претенции.

гр.София,
ул. "Хайдушка гора" 54
+359 890 111 375
office@danaya.bg
www.danaya.bg

(6) Когато няма решение за адекватност (например относно Турция) и трансферът не е такъв по ал. 5, Фондацията преценява дали могат да се приложат подходящи гаранции по чл. 46 от ОРЗД, включително стандартни договорни клаузи на Европейската комисия. При трансфер към болница или друго лечебно заведение в трета държава без решение за адекватност, което обработва данните за свои собствени медицински цели, страните обичайно действат като самостоятелни администратори, поради което приложимият механизъм е Модул 1 — администратор към администратор (Приложение № 14 към настоящата политика). Такъв подход е особено подходящ при повтарящи се трансфери към една и съща болница, партньорска организация или друг получател извън ЕС/ЕИП.

(7) При всеки международен трансфер Фондацията прилага принципите на минимизация, ограничение на целите, поверителност и отчетност - изпращат се само данните и документите, необходими за конкретната цел; когато е възможно, данните за трети лица се заличават или ограничават; използват се защитени канали за комуникация; достъпът се ограничава до конкретни получатели; трансферът се документира.

XVIII. ЛИЧНИ ДАННИ И ИЗКУСТВЕН ИНТЕЛЕКТ

Чл. 60. (1) Фондацията може да използва системи с изкуствен интелект или други автоматизирани инструменти само при спазване на Регламент (ЕС) 2016/679, Закона за защита на личните данни, приложимите актове на Европейския съюз и вътрешните правила на Фондацията.

(2) При използване на системи с изкуствен интелект Фондацията прилага принципите на законосъобразност, прозрачност, минимизиране на данните, ограничение на целите, човешки контрол и защита на данните на етап проектиране и по подразбиране.

(3) Не се допуска въвеждане в публични или неутвърдени AI инструменти на досиета, документи, здравни данни, данни на деца, данни на деца-пациенти, родители, здравни данни, медицински документи, данни за социални услуги, дарители, служители, доброволци, уязвими лица или други лични данни, освен ако това е предварително оценено, документирано и одобрено от Ръководството на Фондацията.

(4) Когато е необходимо използване на AI инструмент за помощни цели, се прилагат анонимизация, псевдонимизация или други мерки за намаляване на риска, а резултатите от инструмента подлежат на човешка проверка.

(5) Използването на AI системи, които могат да породят висок риск за правата и свободите на физическите лица, се допуска само след предварителна оценка на риска и, когато е приложимо, оценка на въздействието върху защитата на данните съгласно Методиката за оценка на риска и оценка на въздействието (Приложение № 15).

XIX. ОТГОВОРНОСТ

Чл. 61. За неизпълнение на задълженията, вменени на съответните оправомощени лица по тази Политика, приложенията към нея, по ЗЗЛД и по Регламент (ЕС) 2016/679, се налагат дисциплинарни наказания по Кодекса на труда, а когато неизпълнението на съответното

гр.София,
ул. "Хайдушка гора" 54
+359 890 111 375
office@danaya.bg
www.danaya.bg

задължение е констатирано и установено от надлежен орган – предвиденото в ЗЗЛД административно наказание.

Чл. 62. (1) За вреди, причинени в резултат на незаконосъобразно обработване на лични данни от служители във Фондация „Даная“, засегнатите лица могат да търсят отговорност от виновните лица по реда на общото гражданско законодателство или наказателна отговорност, ако извършеното представлява престъпление.

(2) Ако в резултат на незаконосъобразно обработване на лични данни, включително незаконното им разкриване или разпространение, са причинени щети на Администратора на лични данни, на виновните лица се търси имуществена отговорност по Кодекса на труда.

XX. ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

Чл. 63. За всички неуредени случаи в настоящата Политика се прилагат разпоредбите на Регламент 2016/679, ЗЗЛД и разпорежданията на Ръководството на Фондация „Даная“ - администратор на лични данни.

Чл. 64. (1) Настоящата Политика и свързаните с нея документи са утвърдени от Ръководството на Фондация „Даная“ и са в сила от …....2026 г., от когато са задължителни за всички служители, сътрудници, доброволци и други лица, които обработват лични данни за или от името на Фондацията. Запознаването с Политиката се удостоверява по подходящ начин.

(2) Настоящата Политика може да бъде променяна и допълвана по всяко време, като промените и допълненията влизат в сила след утвърждаването им от Ръководството на Фондацията.

(3) Неразделна част от системата за управление на защитата на личните данни във Фондацията са и приложенията към настоящата Политика (документи, политики, регистри, методики, споразумения, образци, балансиращи тестове и ОВЗД).

РЕГИСТЪР НА СВЪРЗАНИТЕ ДОКУМЕНТИ И ПРИЛОЖЕНИЯ

1. Политика за обработване и защита на личните данни;

2. Политика за техническите и организационните мерки;

3. Политика за управление на искания от субекти на лични данни;

4. Политика за реагиране на инциденти;

5. Политика за информационна сигурност;

6. Политика за съхраняване и унищожаване на лични данни;

7. Уведомления относно поверителността на личните данни:

гр.София,
ул. "Хайдушка гора" 54
+359 890 111 375
office@danaya.bg
www.danaya.bg

7.1. Уведомление относно поверителността на личните данни за служители и лица на граждански договори;

7.2. Уведомление относно поверителността на личните данни за кандидати за работа;

7.3. Уведомление относно поверителността на личните данни за контрагенти, донори и дарители;

7.4. Уведомление за поверително третиране на личните данни за посетители на сайта, ползватели на онлайн канали и електронната платформа;

7.5. Уведомление относно поверителността на личните данни за нуждаещи се от съдействие, потърсили го по друг начин.

8. Политика за видеонаблюдение;

9. Регистър на дейностите по обработване на лични данни на администратора съгласно чл. 30, параграф 1 от Регламент (ЕС) 2016/679, с приложени необходимите балансиращи тестове;

10.1. Регистър за исканията на субектите на данни;

10.2. Регистър за нарушенията на сигурността на личните данни;

11. Методика за оценка на тежестта на пробиви в сигурността на личните данни (от КЗЛД);

12.1. Споразумение между администратор и обработващ за обработване на лични данни;

12.2. Споразумение между самостоятелни администратори;

13. Образец на заявление за упражняване правата на субект на лични данни;

14. Стандартни договори клази при трансфер, Модул 1 - администратор към администратор;

15. Методика за оценка на риска и оценка на въздействието;

16. Оценка на риска на дейностите по обработване на лични данни;

17. Оценки на въздействието върху защитата на данните.