

София - 1233, жк. "Банишора", ул. „Подполковник Калитин“, бл. 20, тел.: 02 9310779,
факс: 02 8326175, е-майл: badiabet@abv.bg, сайт: www.badiabet.com

Утвърдил:

Майя Викторова Ханджийска –
Председател на УС на
Сдружение „Българска Асоциация Диабет“

**ПОЛИТИКА ЗА ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ В
СДРУЖЕНИЕ С НЕСТОПАНСКА ЦЕЛ ЗА
ОСЪЩЕСТВЯВАНЕ НА ОБЩЕСТВЕНОПОЛЕЗНА ДЕЙНОСТ
„БЪЛГАРСКА АСОЦИАЦИЯ ДИАБЕТ“**

Сдружение с нестопанска цел „Българска Асоциация Диабет /БАД/ („Сдружението“) осъзнава значението на личните данни, тяхната защита и на зачитането на правата на личен живот. Поради тази причина Сдружението и неговите членове и служители следва да опазват поверителността и целостта на всички лични данни, които се съхраняват и обработват от Сдружението или от тях самите, или до които получат достъп, както и да осъществяват дейността си в съответствие с изискванията на българското и европейското законодателство в сферата на защитата на личните данни.

Тази Политика за обработване на личните данни определя основните принципи и изисквания, от които Сдружението и неговите членове и служители следва да се ръководят при работата с лични данни.

I. ОСНОВНИ ПРИНЦИПИ И ОСНОВАНИЯ ЗА ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ

Сдружението обработва лични данни при спазване на следните **основни принципи**:

- ✓ законосъобразност, добросъвестност и прозрачност;
- ✓ ограничение на целите – обработване за конкретни, изрично указани и легитимни цели;

- ✓ свеждане на данните до необходимия минимум - само за целите на обработване;
- ✓ точност – обработване на точни лични данни и в актуален вид;
- ✓ ограничаване на съхранението - във форма позволяваща идентифицирането на субекта и за период не по-дълъг за целите на обработване;
- ✓ цялостност и поверителност – обработване при подходящи технически и организационни мерки за осигуряване на сигурност на личните данни;
- ✓ отчетност – възможност на Сдружение „Българска Асоциация Диабет“ във всеки момент да докаже прилагането на тези принципи.

Сдружение „Българска Асоциация Диабет" обработва лични данни на **законно основание**, което може да бъде:

- ✓ законово задължение на Сдружение „Българска Асоциация Диабет" – съгласно Закон за юридическите лица с нестопанска цел, Правилник за устройството и дейността на Националния съвет за интеграция на хора с увреждания и критериите за представителност на организациите на и за хора с увреждания, Кодекс на труда и подзаконовни нормативни актове, Закон за задълженията и договорите, Закон за обществените поръчки, и др.;
- ✓ съгласие на субекта на данните, което може да бъде оттеглено във всеки един момент, без това да засегне законосъобразността на обработването преди оттеглянето;
- ✓ наличие на легитимен интерес на Сдружение „Българска Асоциация Диабет";
- ✓ във връзка с изпълнение на договор, по който субектът на лични данни е страна или за сключването на такъв, по искане на субекта;
- ✓ във връзка със задача в обществен интерес.

II. ЛИЧНИ ДАННИ, ОБРАБОТВАНИ ОТ СДРУЖЕНИЕТО. ЦЕЛИ И СРОКОВЕ.

Като администратор на лични данни, Сдружението обработва данни на физически лица, включително на членове на сдружения – членове на БАД, с оглед изпълнение на целите, посочени в неговия Устав, на своите служители и кандидатите за работа, кандидатите за изборни длъжности и на представители на свои доставчици, клиенти и контрагенти.

1. Лични данни на физически лица, вкл. членове на сдружения – членове на БАД, с оглед изпълнение на целите, посочени в неговия Устав

Сдружението обработва лични данни на физически лица, вкл. членове на сдружения – членове на БАД, с оглед изпълнение на целите, посочени в неговия Устав, за да идентифицира тези лица и да установи дали те отговарят на изискванията, за да бъдат обхванати от и да участват в програмите и дейностите на Сдружението, като

например Програма „Здравословно хранене в условията на живот с диабет“ и други програми за обучения, семинари, програми за получаване на помощи от медикаменти и помощни средства, финансирани с целева субсидия от държавния бюджет на Република България, респ. да бъдат приети за членове/членове на сдружение-член на Сдружението.

Сдружението обработва лични данни на физически лица, съгласно посоченото по-горе:

Категория лични данни	Цел на обработването	Срок на обработване
1. Три имена	<ul style="list-style-type: none"> - идентифициране на лицето - да установи дали лицето отговаря на изискванията, за да бъде обхванато от програмите и дейностите на Сдружението - да бъде прието за член на Сдружението/член на сдружение-член - регистрация в събития, организирани от Сдружение „Българска Асоциация Диабет“ 	<ul style="list-style-type: none"> - активно до приключване изпълнението на съответната програма и впоследствие, до изтичане на законоустановените срокове за съхранение на документацията по съответната програма, включително документация и договор за обществена поръчка - постоянно – от възникване до прекратяване на членство и изтичане на законоустановените срокове за съхранение на информация и документи, съдържащи информация за членовете на Сдружението/членовете на Сдружението - за времето от регистрацията в съответното събитие до неговото приключване, включително отчитане на дейностите и резултатите от него, ако това се изисква, и впоследствие, до изтичане на законоустановените срокове за съхранение на документацията по съответното

Категория лични данни	Цел на обработването	Срок на обработване
		събитие
2. ЕГН	- идентифициране на лицето	Съобразно посоченото в т. 1 от настоящата таблица.
3. Постоянен адрес	- контакт с лицето	Съобразно посоченото в т. 1 от настоящата таблица.
4. Телефон и/или имейл	- контакт с лицето - изпращане на информационни съобщения	Съобразно посоченото в т. 1 от настоящата таблица.
5. Данни от лична карта (паспортни данни)	- идентифициране на лицето	Съобразно посоченото в т. 1 от настоящата таблица.
6. Данни за здравословно състояние (наличие на заболяване диабет) - копие от рецептурна книжка заверено от Здравна каса или епикризи, или други документи удостоверяващи заболяване от диабет.	- да установи дали лицето отговаря на изискванията, за да бъде обхванато от програмите и дейностите на Сдружението	Съобразно посоченото в т. 1 от настоящата таблица.
7. Данни за семейно положение	- да установи дали лицето отговаря на изискванията, за да бъде обхванато от програмите и дейностите на Сдружението (напр. за установяване правата на непълнолетен/малолетен член на семейство за участие по програми, реализирани от Сдружението).	Съобразно посоченото в т. 1 от настоящата таблица.
8. Снимки от събития и инициативи на	Промотиране дейността на Сдружението.	Постоянно съхранение до прекратяване на Сдружението,

Категория лични данни	Цел на обработването	Срок на обработване
Сдружението	Споделяне в социални мрежи на снимки от участия на спортни мероприятия, благотворителни инициативи и други подобни.	освен ако лицето оттегли съгласието си преди това.

Сдружението не предоставя горепосочените лични данни на друго лице или трета държава, освен в законово определени случаи на компетентни за това органи или с изрично писмено съгласие на субекта, при участие в международни програми и проекти.

2. Лични данни на служители на Сдружението, на лица на изборните длъжности в УС и КС на БАД и кандидати за работа/изборни длъжности

Сдружението обработва лични данни на свои служители и на изборните длъжности в УС и КС на БАД, както следва:

Категория лични данни	Цел на обработването	Срок на обработване
1. Три имена	<ul style="list-style-type: none"> - идентифициране на лицето - изпълнение на законови задължения за деклариране на данни за трудовото правоотношение пред НАП, НОИ, Инспекция по труда, Агенция по заетостта, както и изпълнение на други задължения във връзка с трудовото правоотношение. - идентифициране на кандидат за член на УС и КС на БАД - изпълнение на изискванията на Устава и ЗЮЛНЦ за участие в управителен и контролен орган на БАД. 	<ul style="list-style-type: none"> - постоянно съхранение до прекратяване на Сдружението и предаване на данните в архивите на НОИ - за избраните членове на УС и КС на БАД – до изтичане на мандата на съответния съвет/член и впоследствие, до изтичане на законоустановените срокове за съхранение на документация на Сдружението, съдържаща

Категория лични данни	Цел на обработването	Срок на обработване
		данните на членовете на УС и КС на БАД, чийто мандат е изтекъл
2. ЕГН	<ul style="list-style-type: none"> - идентифициране на служителя - изпълнение на законови задължения за деклариране на данни за трудовото правоотношение пред НАП, НОИ, Инспекция по труда, Агенция по заетостта, както и изпълнение на други задължения във връзка с трудовото правоотношение - идентифициране на кандидат за член на УС и КС на БАД - изпълнение на изискванията на Устава и ЗЮЛНЦ за участие в управителен и контролен орган на БАД . 	<ul style="list-style-type: none"> - постоянно съхранение до прекратяване на Сдружението и предаване на данните в архивите на НОИ - за избраните членове на УС и КС на БАД – до изтичане на мандата на съответния съвет/член и впоследствие, до изтичане на законоустановените срокове за съхранение на документация на Сдружението, съдържаща данните на членовете на УС и КС на БАД, чийто мандат е изтекъл.
3. Постоянен адрес	<ul style="list-style-type: none"> - идентифициране на служителя - изпълнение на законови задължения за деклариране на данни за трудовото правоотношение пред НАП, НОИ, Инспекция по труда, Агенция по заетостта, както и изпълнение на други задължения във връзка с трудовото правоотношение. - идентифициране на кандидат за член на УС и КС на БАД - изпълнение на изискванията на Устава и ЗЮЛНЦ за участие в управителен и контролен орган на БАД 	<ul style="list-style-type: none"> - постоянно съхранение до прекратяване на Сдружението и предаване на данните в архивите на НОИ - за избраните членове на УС и КС на БАД – до изтичане на мандата на съответния съвет/член и впоследствие, до изтичане на законоустановените срокове за съхранение на документация на Сдружението, съдържаща данните на членовете на УС и КС на БАД, чийто мандат е изтекъл

Категория лични данни	Цел на обработването	Срок на обработване
4. Телефон и/или имейл	<ul style="list-style-type: none"> - контакт със служителя - контакт с член на УС и КС 	<ul style="list-style-type: none"> - до прекратяване на трудовото правоотношение - за избраните членове на УС и КС на БАД – до изтичане на мандата на съответния съвет/член
5. Данни от лична карта (паспортни данни)	<ul style="list-style-type: none"> - идентифициране на служителя - изпълнение на законови задължения за деклариране на данни за трудовото правоотношение пред НАП, НОИ, Инспекция по труда, Агенция по заетостта, както и изпълнение на други задължения във връзка с трудовото правоотношение. - идентифициране на кандидат за член на УС и КС на БАД - изпълнение на изискванията на Устава и ЗЮЛНЦ за участие в управителен и контролен орган на БАД . 	<ul style="list-style-type: none"> - постоянно съхранение до прекратяване на Сдружението и предаване на данните в архивите на НОИ - за избраните членове на УС и КС на БАД – до изтичане на мандата на съответния съвет/член и впоследствие, до изтичане на законоустановените срокове за съхранение на документация на Сдружението, съдържаща данните на членовете на УС и КС на БАД, чийто мандат е изтекъл
6. Образователна степен, специалност и академични резултати	<ul style="list-style-type: none"> - установяване дали лицето отговаря на изискванията за заемане на длъжността - изпълнение на изискванията на Устава и ЗЮЛНЦ за участие в управителен и контролен орган на БАД 	<ul style="list-style-type: none"> - до прекратяване на трудовото правоотношение - за избраните членове на УС и КС на БАД – до изтичане на мандата на съответния съвет/член
7. Номер на диплома и дата на издаване	<ul style="list-style-type: none"> - установяване дали лицето отговаря на изискванията за заемане на длъжността 	до прекратяване на трудовото правоотношение
8. Трудов стаж	<ul style="list-style-type: none"> - установяване дали лицето отговаря на изискванията за заемане на длъжността - определяне на трудов стаж за професионален опит 	до прекратяване на трудовото правоотношение

Категория лични данни	Цел на обработването	Срок на обработване
	- описване на трудовото правоотношение със Сдружението	
9. Данни (IBAN) за банковата сметка на служителя	- изплащане на трудови възнаграждения и обезщетения от НОИ на служителите по банков път	До прекратяване на трудовото правоотношение и/или до изплащане на всички задължения за периоди, предшестващи прекратяването
10. Размер на трудовото възнаграждение	- изплащане на трудови възнаграждения - предоставяне на информация до НАП, НОИ, Инспекция по труда (ИТ), Агенция по заетостта (АЗ)	Постоянно съхранение до прекратяване на Сдружението и предаване на данните в архивите на НОИ
11. Данни за здравословното състояние	- установяване съществуването на законовите предпоставки за ползване на платен отпуск поради заболяване и/или бременност, раждане или трудоустрояване - изчисляване размера на трудовото възнаграждение - закрила при уволнение в определените от трудовото законодателство случаи	3 години, считано от 1 януари на годината, следващата годината на издаване на болничния лист
12. Трафични данни – данни за трафика от/към служебни мейл адреси	- осигуряване сигурността на вътрешните комуникации и системи на Сдружението, защита от вируси и други злонамерени програми	до 3 месеца
13. Снимки на служители или членове на УС и КС на БАД от събития и инициативи на Сдружението	Промотиране дейността на Сдружението в интернет. Споделяне в социални мрежи на снимки от участия на обучителни, спортни мероприятия, благотворителни инициативи и други подобни.	постоянно съхранение до прекратяване на Сдружението, освен ако лицето не оттегли съгласието си преди това
14. Снимка на служителя в личния картон	- идентифициране на служителя	до прекратяване на трудовото правоотношение

Сдружението получава лични данни на кандидатите за работа/за избор за

членове на УС и КС, каквито те са му предоставили в документите за кандидатстване, но доколкото това е нужно за целите на подбора, то обработва само данните по точки 1, 3, 4 и 6-8. В случай, че съответният кандидат бъде одобрен и бъде сключен договор със Сдружението, то започва да обработва личните му данни съгласно посоченото по-горе за служителите на Сдружението. Ако кандидатът не бъде одобрен, Сдружението съхранява изпратените от него лични данни, както следва: (а) ако кандидатстването не е по конкретна обява - за срок до 2 месеца от постъпването им в Сдружението с цел разглеждане на кандидатурата и контакт с кандидата, ако се открие подходяща за него/нея позиция, или (б) ако кандидатстването е по конкретна позиция - за периода на подбора за съответната позиция (в) ако кандидатстването е за членове на УС и КС – до 1 една година от провеждане на избора на членове за УС и КС – с цел съхранение на цялата документация от провеждане на общо събрание при евентуални съдебни спорове /арг. Чл. 25, ал. 5 от ЗЮЛНЦ/.

Сдружението може да предоставя лични данни на свои служители и на членове на УС и КС на компетентните държавни органи по предвидения в закона ред и в случаите, когато е налице съответно задължение за предоставянето им. Извън тези случаи, Сдружението може да предоставя лични данни на служители на трети лица, както следва:

- ✓ Данни по лична карта (напр. три имена и ЕГН, когато е необходимо) – (а) на авиолинии или други превозвачи и/или доставчици на хотелиерски услуги във връзка с изпращане в командировки; и (б) на частни съдебни изпълнители във връзка с реализирането на легитимните интереси на Сдружението в случай на дължими от служителя суми;
- ✓ Имена, телефон и e-mail адрес за контакт – на трети лица, доставчици или партньори на Сдружението, с оглед изпълнението на договорите между Сдружението и такива трети лица, когато трудовите задължения на служителя са свързани с това;
- ✓ Други данни и лица, извън посочените по-горе – след уведомяването на съответния служител и получаване на съгласие, когато е приложимо.

3. Представители на доставчици, партньори и други контрагенти

Сдружението обработва лични данни на представители (лица за контакт) на свои доставчици, участници в процедури за възлагане на обществени поръчки, партньори и други контрагенти, доколкото това е необходимо за осъществяване дейността на Сдружението и единствено за целите на изпълнението на договорите със съответните лица.

Категория лични данни	Цел на обработването	Срок на обработването
1. Три имена	- комуникация с доставчика/контрагента	Активно, до прекратяване на договорното взаимоотношение.

Категория лични данни	Цел на обработването	Срок на обработването
		Последващо архивиране и съхранение в законоустановените срокове за съхранение на счетоводни документи или съхранение на документи по ЗОП.
2. Данни за контакт (телефон, мейл адрес)	- комуникация с доставчика/ контрагента	Активно, до прекратяване на договорното взаимоотношение. Последващо архивиране и съхранение на в законоустановените срокове за съхранение на счетоводни документи или съхранение на документи по ЗОП.
3. Други данни, които се изискват от ЗОП	- сключване, изпълнение и администриране на обществени поръчки	Активно, до прекратяване на договорното взаимоотношение. Последващо архивиране и съхранение на документацията в законоустановените срокове за съхранение на документи по ЗОП.

Сдружението може да предоставя лични данни на представители на свои контрагенти на компетентните държавни органи по предвидения в закона ред и в случаите, когато е налице съответно задължение за предоставянето им. Извън тези случаи, Сдружението не предоставя на трети лица такива лични данни на представители без тяхното знание и съгласие, когато е приложимо.

III. ПРАВА НА СУБЕКТИТЕ НА ЛИЧНИ ДАННИ

Сдружението предприема мерки за реализиране правата на всички лица, чиито данни обработва, в съответствие с условията за тяхното упражняване съгласно българското и европейското законодателство.

В съответствие с Общия Регламент за защита на личните данни (ЕС 2016/679) („Регламента“), субектите на данните имат следните права:

1. Право да бъдат информирани

Сдружението предоставя на субектите на данните подробна информация съобразно изискванията на Регламента, включително за видовете лични данни, които обработва, целите и сроковете на обработване и третите лица, на които могат да бъдат предоставяни.

Когато Сдружението, в качеството си на администратор на лични данни, обработва лични данни, които не са получени директно от субекта им, то предоставя изискваната от Регламента информация:

- а. в разумен срок след получаването на личните данни, но най-късно в срок до един месец, като се отчитат конкретните обстоятелства, при които личните данни се обработват;
- б. ако данните се използват за контакт със субекта на данните, най-късно при осъществяване на първия контакт с този субект на данните; или
- в. ако е предвидено разкриване пред друг получател, най-късно при разкриването на личните данни за първи път.

2. Право на достъп до личните данни

Всеки субект на данни има право да получи от Сдружението потвърждение дали се обработват лични данни, свързани с него, и ако това е така, да получи достъп до тях, както и до друга информация, определена в чл. 15 от Регламента.

3. Право на коригиране на личните данни

Всеки субект на данни има право да поиска от Сдружението да коригира без ненужно забавяне неточните лични данни, свързани с него/нея. Като се имат предвид целите на обработването субектът на данните има право непълните лични данни да бъдат допълнени, включително чрез посочването им в декларация, изпратена до Сдружението.

4. Право на изтриване

Всеки субект на данни има право да поиска от Сдружението да изтрие негови лични данни при предпоставките, посочените в чл. 17 от Регламента, включително в случаи, когато обработването се осъществява въз основа на съгласие на субекта и това съгласие бъде оттеглено; когато съответните лични данни повече не са необходими за целите, за които са били обработвани или когато обработването им е неправомерно.

5. Право на ограничаване на обработването

Всеки субект на данни има право да поиска от Сдружението временно преустановяване/ограничаване на обработването на неговите лични данни съгласно чл. 18 от Регламента, когато оспорва тяхната точност/актуалност; когато обработването им е неправомерно, но субектът на данните не желае да бъдат изтрити; когато Сдружението не се нуждае повече от личните данни за целите на обработването, но

субектът на данните ги изисква за установяването, упражняването или защитата на правни претенции или когато субектът на данните е възразил срещу тяхното обработване съгласно т.б по-долу и очаква проверка по неговото възражение.

6. Право на възражение срещу обработването

Всеки субект на лични данни има право да възрази срещу обработването на неговите данни от страна на Сдружението, когато правното основание за обработването на данните му са легитимни интереси на Сдружението или изпълнение на задача от обществен интерес. В този случай Сдружението следва да преустанови обработването освен ако съществуват убедителни законови основания за обработването, които имат предимство пред интересите, правата и свободите на субекта.

7. Право на преносимост на личните данни

Всеки субект на лични данни има право да получи личните данни, които го засягат и които той е предоставил на Сдружението, в структуриран и пригоден за машинно четене формат и има правото да прехвърли тези данни на друг администратор без възпрепятстване от Сдружението, когато обработването на данните се извършва въз основа на съгласието на субекта или на основание изпълнение на договорни задължения от страна на Сдружението.

Упражняване на правата на субектите на лични данни

Сдружението предоставя възможност на субектите на личните данни да реализират своите права съгласно Регламента, като се обърнат с искане към **Длъжностно лице по защита на данните („ДЛЗД“)** на следния адрес: гр. София, ж.к. „Банишора“, ул. „Подполковник Калитин“, бл. 20, тел. 02 9310779, факс 02 8326175, на вниманието на Длъжностното лице по защита на данните, респективно на адреса на ел. поща: dpo-badiabet@abv.bg. Действията, които ДЛЗД и подпомагащите го служители на Сдружението следва да извършат при постъпване на искане за упражняване на права, са уредени в отделна процедура, приета от Сдружението. ДЛЗД и подпомагащите го служители на Сдружението са длъжни да се запознаят и да спазват процедурата по предходното изречение.

IV. ТЕХНИЧЕСКИ И ОРГАНИЗАЦИОННИ МЕРКИ. УНИЩОЖАВАНЕ НА ДАННИТЕ

Сдружение „Българска Асоциация Диабет“ осигурява подходящи технически и организационни мерки за обработване на личните данни съобразно нормативно установените задължения, като взетите мерки (по подразбиране) гарантират, че:

- ✓ се обработват лични данни само за конкретна цел на обработването (с оглед обем на лични данни, степен на обработване, период на съхранение и достъпност);
- ✓ до данните нямат достъп неограничен брой лица (без да е необходима

допълнителна намеса от физическо лице).

Информацията, съдържаща лични данни на хартиен носител се съхранява в папки, които се подреждат в специални картотечни шкафове в заключени помещения. Правата и задълженията на служителите за работа с тях са регламентирани в длъжностните им характеристики. Правата и задълженията на други обработващи лични данни се регламентират в договор. Предоставянето, промяната или прекратяването на оторизиран достъп до регистрите на хартиен носител се контролира от Председателя на УС на БАД.

Картотечният шкаф може да бъде поставен в помещение, предназначено за самостоятелна работа на лицата, обработващи лични данни или в общо помещение за работа с изпълняващи други дейности, което се заключава.

Достъп до личните данни има само лицето, което обработва лични данни, като то не трябва да предоставя достъп до предоставените му за обработка данни на трети лица, освен в предвидените от закона случаи.

Възможността за предоставяне другиму достъп до личните данни при обработката им е ограничена и изрично е регламентирана законово.

Формата на организация и съхраняване на личните данни на технически носител се осъществява чрез тяхното въвеждане на твърд диск на сървъри от компютърната мрежа (в случай, че се обработват от повече от един служител) или на изолиран компютър (в случай, че се обработват само от един служител или от съответното работно място не може да бъде осигурен достъп до сървър). Компютърът е със защитен достъп до личните данни, с който може да работи само обработващият лични данни и мерки при средно ниво, съобразно изискванията на Наредба № 1 от 30.01.2013 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни.

При работа с данните се използват съответните софтуерни продукти за обработка. Те могат да бъдат адаптирани към специфичните нужди на администратора на лични данни. Данните се въвеждат в компютъра от хартиен носител.

Достъп до файловете за обработка на лични данни имат само работещите с лични данни. Носители с лични данни могат да се разпространяват само ако данните са криптирани или ако е използван друг механизъм, гарантиращ, че данните не могат да се четат или променят при пренасянето им.

Защита на електронните данни от неправомерен достъп, повреждане, изгубване или унищожаване се осигурява посредством поддържане на антивирусни програми, периодично архивиране на данните на отделни електронни носители, както и чрез съхраняване на информацията на хартиен носител. Когато данните се намират на изолирани компютри архивирането им се извършва от оператора на съответния компютър (обработващия лични данни).

Администраторът на лични данни предприема необходимите технически и организационни мерки, за да защити данните от случайно или незаконно унищожаване, или от случайна загуба, от неправомерен достъп, изменение или разпространение, както и от други незаконни форми на обработване, съобразно изискванията на Наредба № 1 от 30.01.2013 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни.

Администраторът взема специални мерки за защита чрез криптиране, когато обработването включва предаване на данните по електронен път.

Мерките за гарантиране нивото на сигурност:

1. компютърните работни конфигурации да използват Desktop операционни системи съобразно изискванията на приложния софтуер за работа с лични данни, да са компетентно балансирани и функционално оптимизирани;
2. минималния набор от системни програмни средства на всяка работна компютърна конфигурация включва:
 - Операционна система съобразно изискванията на ползвания приложен софтуер с инсталирани последни пакети за сигурност;
 - Антивирусен софтуер с включено автоматично обновяване и постоянно сканиране;
 - Активирана защитна стена и деинсталирани комуникатори, осигуряващи достъп извън рамките на компютърната мрежа на БАД и създаващи предпоставки за идентифициране на IP адрес на потребителя и за достъп на злонамерен софтуер и мобилен код до компютрите;

Физически мерки за гарантиране нивото на сигурност:

1. в помещенията, в които са разположени компютърни и комуникационни средства, е осигурена система за ограничаване на достъпа;
2. всички работни помещения се заключват извън рамките на установеното работно време и достъпът до тях е регламентиран. Всички магнито-оптични носители, които се използват за запис на лични данни в резултат на архивиране и изготвяне на копия на базите данни, се предават и съхраняват в шкаф, който се заключва.

Организационни мерки за гарантиране нивото на сигурност:

1. охраната на работните помещения се осъществява чрез СОТ.
2. работните компютърни конфигурации, както и цялата IT инфраструктура, включително и достъпът до интернет, се използват единствено за служебни цели;
3. проверка на всички работни компютърни конфигурации по чл. 8 от Наредба № 1 от 30.01.2013 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни;
4. пренасянето на лични данни през (чрез) интернет се осъществява чрез електронна поща;
5. при ремонт на компютърна техника, на която се съхраняват лични данни, предоставянето ѝ на сервизната организация се извършва без устройствата, на които се съхраняват лични данни.

След изтичането на сроковете за обработване на лични данни, посочени в тази Политика, или при отпадане на основанието за това обработване, включително последващо съхранение, служителите на Сдружението, работещи със съответните данни, са длъжни да ги унищожават, както следва:

- ✓ данни на хартиен носител: хартиените носители се унищожават от оторизирани за тази дейност организации или със специално предназначени за целта уреди (шредери), които Сдружението осигурява. Когато на съответния хартиен носител се съдържат и други данни, които все още се обработват от Сдружението, ненужните данни се заличават от хартиения носител със средства, непозволяващи тяхното възстановяване;
- ✓ данни на електронен носител (твърд диск, флаш памет, сървър и пр.): ненужните данни се заличават по траен начин от всички системи и бекъп копия на Сдружението.

След унищожаване на лични данни, чиито срок на съхранение е изтекъл, съответният служител на Сдружението попълва и предава на ДЛЗД протокол за извършеното унищожаване, в който посочва своите имена, вида на изтритите лични данни (без да посочва конкретно самите данни) и метода, по който са изтрити. При ангажиране на оторизирана организация, представител на същата попълва и предава на ДЛЗД протокол за извършеното унищожаване, в който посочва своите имена, вида на изтритите лични данни (без да посочва конкретно самите данни) и метода, по който са изтрити. ДЛЗД съхранява протоколите за унищожаване на данни в отделен регистър.

V. НАРУШЕНИЕ НА СИГУРНОСТТА НА ДАННИТЕ

В случай на нарушение на сигурността на личните данни Сдружението, без ненужно забавяне и когато това е осъществимо — не по-късно от 72 часа след като нарушението е установено, уведомява за него Комисията за защита на личните данни.

При възникване и установяване на инцидент веднага се докладва на Председателя на УС на Сдружението и се предприемат незабавни подходящи технически и организационни мерки за защита по отношение на данните и за отстраняване на нарушението.

При бедствия и аварии се предприемат следните действия:

1. защита при аварии– предприемат се конкретни действия в зависимост от конкретната ситуация;
2. защита от пожари - незабавно гасене със собствени средства /пожарогасители/и уведомяване на съответните органи;
3. защита от наводнения - предприемат действия по ограничаване на разпространението, както и се изпомпва вода или се загребва със собствени подръчни средства.

При установяване на нарушение на сигурността на личните данни, което може да породи висок риск за правата и свободите, Сдружение „Българска Асоциация Диабет“ уведомява субекта на лични данни без ненужно забавяне за нарушението, както и за мерките, които са предприети или предстои да бъдат предприети.

Сдружение „Българска Асоциация Диабет“ не уведомява субекта на лични данни, ако:

- ✓ е предприело подходящи технически и организационни мерки за защита по отношение на данните, засегнати от нарушението на сигурността;
- ✓ е взело впоследствие мерки, които гарантират, че нарушението няма да доведе

- до висок риск за правата на субекта на лични данни;
- ✓ уведомяването би изисквало непропорционални усилия

За Сдружение с нестопанска цел „Българска Асоциация Диабет“

Майя Викторова Ханджийска – Председател на УС

Подпис: _____

Дата: