

**ПРАВИЛА (ПОЛИТИКА) ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ  
НА  
ФОНДАЦИЯ “ФОНДАЦИЯ “БЪЛГАРСКА АСОЦИАЦИЯ ЗА БИОЛОГИЯ НА  
ОСТАРЯВАНЕТО””**

**ГЛАВА I. ОБЩИ ПОЛОЖЕНИЯ**

**Чл. 1.** С настоящите правила за защита на личните данни (“Правилата”) се определят политиката и необходимите технически и организационни мерки за защита на личните данни на членовете, участниците в събития, контрагентите и служителите на фондация “Фондация “Българска асоциация за биология на остаряването””, ЕИК 208526837, със седалище и адрес на управление: гр. София, п.к. 1000, район “Триадица”, ул. “Кърниградска” № 19, ет. 1 (“Фондацията”), съгласно Регламент (ЕС) № 2016/679 на Европейския Парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни (**ОРЗД**), Закона за защита на личните данни (**ЗЗЛД**) и всички други приложими подзаконовни нормативни актове.

**Чл. 2.** (1) Настоящите правила са задължителни за всички служители на Фондацията и са насочени към осигуряване на адекватно ниво на защита на поддържаните регистри с лични данни от случайно или незаконно унищожаване, от случайна загуба, от неправомерен достъп, изменение или разпространение, както и от други незаконни форми на обработване.

(2) С Правилата се информират служителите на Фондацията, нейните контрагенти, лицата, използващи услугите на Фондацията и всички трети лица, чиито лични данни Фондацията може да събира и обработва, независимо от основанието за това, за правата им като субекти на лични данни съгласно ОРЗД. С правилата Фондацията цели също така да приложи мерки, които отговарят по-специално на принципите за защита на данните на етапа на проектирането и защита на данните по подразбиране, които мерки се изразяват, наред с другото, в свеждане до минимум на обработването на лични данни, псевдонимизиране на лични данни на възможно най-ранен етап, прозрачност по отношение на функциите и обработването на лични данни, създаване на възможност за субекта на данни за достъп до обработваните данни, възможност за Фондацията да създава и подобрява елементи на сигурността.

**Чл. 3.** Всички обработвани лични данни ще бъдат третирани като строго поверителни. Основните принципи, които се прилагат от Фондацията при обработването на лични данни са:

1. законосъобразност, добросъвестност и прозрачност през целия процес на обработване на лични данни;
2. ограничение на целите - личните данни, които Фондацията обработва, се събират за конкретни, изрично указани и легитимни цели и не се обработват по начин, несъвместим с тези цели;

3. Фондацията свежда до минимум личните данни, които обработва, и те се ограничават до такива, необходими за целите, за които се обработват, без да изисква излишни данни;
4. точност при обработването – Фондацията поддържа в актуален вид личните данни, които обработва, и предприема всички разумни мерки, за да се гарантира своевременното изтриване или коригиране на неточни лични данни, като се имат предвид целите, за които те се обработват;
5. ограничение на съхранението – личните данни се съхраняват във форма, която позволява идентифицирането на субекта на данните за период, не по-дълъг от необходимото за целите, за които се обработват, като се вземат предвид всички приложими нормативни срокове и разпоредби, които Фондацията трябва да спазва;
6. цялостност и поверителност – личните данни се обработват по начин, който гарантира подходящо ниво на сигурност, включително защита срещу неразрешено или незаконосъобразно обработване и срещу случайна загуба, унищожаване или повреждане, като се прилагат подходящи технически или организационни мерки.

**Чл. 4.** Съгласно настоящите Правила:

1. „лични данни” означава всяка информация, отнасяща се до физическо лице, което е идентифицирано или може да бъде идентифицирано пряко или непряко по-специално чрез идентификатор като име, идентификационен номер, данни за местонахождение, телефон или по един или повече специфични признаци;
2. „обработване на лични данни” е всяко действие или съвкупност от действия, които могат да се извършват по отношение на личните данни с автоматични или други средства, като събиране, записване, организиране, структуриране, съхраняване, адаптиране, извличане, употреба, разпространяване, комбиниране, ограничаване, изтриване или унищожаване;
3. „регистър на лични данни” е всеки структуриран набор от лични данни, достъпът до който се осъществява съгласно определени критерии.

## **ГЛАВА II. ОБЩО ОПИСАНИЕ НА ПОДДЪРЖАНИТЕ РЕГИСТРИ. КАТЕГОРИИ ЛИЧНИ ДАННИ И ОСНОВАНИЕ ЗА ОБРАБОТВАНЕ**

**Чл. 5.** Фондацията въвежда подходящи технически и организационни мерки, за да се гарантира, че по подразбиране се обработват само лични данни, които са необходими за всяка конкретна цел на обработването. Това задължение се отнася до обема на събраните лични данни, степента на обработването, периода на съхраняването им и тяхната достъпност. По-специално, подобни мерки гарантират, че по подразбиране без намеса от страна на физическото лице, личните данни не са достъпни за неограничен брой физически лица.

**Чл. 6.** (1) Във Фондацията са обособени четири регистъра за лични данни в зависимост от целите на обработка:

1. Регистър “Членове на Фондацията”;
2. Регистър “Участници в събития и лица, ползващи услугите на Фондацията”;
- а. Регистър „Контрагенти”;
3. Регистър „Доставчици”;
4. Регистър „Служители”.

(2) Съветът на настоятелите отговаря за воденето, поддържането и съхранението на всички регистри на Фондацията.

### **Регистър “Членове на Фондацията”**

**Чл. 7.** В регистър “Членове на Фондацията” се набират и съхраняват лични данни на физическите лица – членове на Фондацията, както и на физическите лица, представляващи юридическите лица – членове на Фондацията. Регистърът се води по електронен път.

**Чл. 8.** (1) Личните данни, които членовете на Фондацията предоставят на Фондацията, могат да включват:

1. имейл адрес;
2. име и фамилия;
3. телефонен номер или електронен адрес за връзка;
4. настоящ адрес (населено място);
5. националност;
6. информация относно образование или професия;
7. пол, възраст, здравен статус.

(2) Личните данни се събират чрез попълване на съответен формуляр онлайн или на място. Гореописаните лични данни се събират, за да може да се извърши идентификация на физическите лица, която Фондацията е задължена да извърши по закон, както и за допълнителна сигурност на самите физически лица, а също и с оглед естеството на предлаганите им услуги, когато техният вид зависи от специфични данни за личността на ползвателите им.

(3) Събраните лични данни от регистър “Членове на Фондацията” се използват за следните цели:

1. осигуряване на участието на члена в събитие, посветено на постигането на цели, попадащи в обхвата на целите на Фондацията, като например свързване на глобалната общност на българските професионалисти в областта на дълголетието; създаване на мрежа от български професионалисти, изследователи и ентузиастични в науката за дълголетието по целия свят; подтикване на новаторски изследвания и технологично развитие за удължаване на здравословния живот в България и по света; въздействие на държавните

политики и общественото отношение към стареенето, с цел България да се превърне в един от водещите центрове в Европа в науката и да се създадат условия за развитие на индустрията на дълголетието; насърчаване на млади изследователи и на изграждането на връзки както между тях, така и с водещите в областта на дълголетието международни организации и институти; промотиране на обучение през целия живот и обществена осведоменост за дълголетието; промяна на общественото отношение към осъзнаване на възможностите за дълголетието и смисълът от него или сродни или свързани с една или повече от тях цели;

2. предоставяне на информация и други услуги в рамките на обхвата на дейността на Фондацията, а когато това е необходимо – и след получаване на съответно разрешение;

3. спазване на законово задължение, което се прилага спрямо Фондацията;

4. обработването на лични данни е необходимо за целите на законните интереси, преследвани от Фондацията.

**Чл. 9.** Фондацията създава и поддържа регистър “Членове на Фондацията”.

**Чл. 10.** Достъпът до личните данни е оторизиран и е възможен само за членовете на Съвета на настоятелите и тези служители на Фондацията, за които това е необходимо за изпълнение на служебните им задължения.

**Чл. 11.** Копирането на документи на хартиен носител или използването на записващи устройства, които позволяват копирането на документи на електронен носител, е позволено само за целите на изпълнение на задълженията на членовете на Съвета на настоятелите и на служителите на Фондацията, като например изпращане на данни към административни и контролни органи посредством електронен подпис.

#### **Регистър “Участници в събития и лица, ползващи услугите на Фондацията”**

**Чл. 12.** В регистър “Участници в събития и лица, ползващи услугите на Фондацията” се набират и съхраняват лични данни на участниците в събития – физически лица. Регистърът се води по електронен път.

**Чл. 13. (1)** Личните данни, които участниците в събития предоставят преди или при участие в събитие или ползване на услуга, предоставяна от Фондацията, могат да включват:

1. имейл адрес;
2. име и фамилия;
3. телефонен номер или електронен адрес за връзка;
4. настоящ адрес (населено място);
5. националност;
6. информация относно образование или професия;

7. пол, възраст, здравен статус.

(2) Личните данни се събират чрез попълване на съответен формуляр онлайн или на място. Гореописаните лични данни се събират, за да може да се извърши идентификация на физическите лица, която Фондацията е задължена да извърши по закон, както и за допълнителна сигурност на самите физически лица, а също и с оглед естеството на предлаганите им услуги, когато техният вид зависи от специфични данни за личността на ползвателите им.

(3) Събраните лични данни от регистър “Участници в събития и лица, ползващи услугите на Фондацията” се използват за следните цели:

1. осигуряване на участието на участника в събитие, посветено на постигането на цели, попадащи в обхвата на целите на Фондацията, като например свързване на глобалната общност на българските професионалисти в областта на дълголетие; създаване на мрежа от български професионалисти, изследователи и ентузиастични в науката за дълголетие по целия свят; подтикване на новаторски изследвания и технологично развитие за удължаване на здравословния живот в България и по света; въздействие на държавните политики и общественото отношение към стареенето, с цел България да се превърне в един от водещите центрове в Европа в науката и да се създадат условия за развитие на индустрията на дълголетие; насърчаване на млади изследователи и на изграждането на връзки както между тях, така и с водещите в областта на дълголетие международни организации и институти; промотиране на обучение през целия живот и обществена осведоменост за дълголетие; промяна на общественото отношение към осъзнаване на възможностите за дълголетие и смисълът от него или сродни или свързани с една или повече от тях цели;

2. предоставяне на информация и други услуги в рамките на обхвата на дейността на Фондацията, а когато това е необходимо – и след получаване на съответно разрешение;

3. спазване на законово задължение, което се прилага спрямо Фондацията;

4. обработването на лични данни е необходимо за целите на законните интереси, преследвани от Фондацията.

**Чл. 14.** Фондацията създава и поддържа регистър “Участници в събития и лица, ползващи услугите на Фондацията”.

**Чл. 15.** Достъпът до личните данни е оторизиран и е възможен само за членовете на Съвета на настоятелите и за тези служители на Фондацията, за които това е необходимо за изпълнение на служебните им задължения.

**Чл. 16.** Копирането на документи на хартиен носител или използването на записващи устройства, които позволяват копирането на документи на електронен носител, е позволено само за целите на изпълнение на задълженията на членовете на

Съвета на настоятелите и на служителите на Фондацията, като например изпращане на данни към административни и контролни органи посредством електронен подпис.

### **Регистър „Доставчици”**

**Чл. 17.** Фондацията сключва договори за доставка на стоки и услуги с различни доставчици за целите на изпълнение на предмета на своята дейност. В този регистър се набират и съхраняват данни за доставчиците на стоки и услуги на Фондацията. В случаите когато Фондацията предоставя лични данни на свои доставчици, Фондацията осигурява спазване на ОРЗД чрез сключване на допълнителни споразумения към съществуващите договорни отношения.

**Чл. 18.** Регистър „Доставчици” се поддържа на електронен носител и включва идентифициращи данни за съответния контрагент (като име, ЕИК/ЕГН или друг регистрационен номер (ако е приложим), адрес за кореспонденция, имейл на лице за контакт, телефон, предмет на договора, срок за изпълнение/доставка). В регистъра се съдържат и лични данни като имена на съответните физически лица, ЕГН, телефон, имейл и адрес за кореспонденция за доставчиците на Фондацията, които са физически лица, с цел тяхната идентификация и спазване на приложимото данъчно законодателство. Такива доставчици са ограничен кръг от физически лица и са изключение в ежедневната практика на Фондацията.

**Чл. 19.** Събраните лични данни се използват за следните цели:

1. индивидуализиране на договорните правоотношения - обработването е необходимо за изпълнението на договор, по който субектът на данни (физическото лице) е страна;
2. спазване на законово задължение, което се прилага спрямо Фондацията;
3. използване на събраните данни за служебни цели, свързани със съществуването, изменението и прекратяването на договорните правоотношения с доставчиците, воденето на счетоводна отчетност и др.

### **Регистър „Контрагенти”**

**Чл. 20.** Фондацията създава и поддържа Регистър „Контрагенти”.

**Чл. 21.** Достъпът до личните данни в Регистър „Контрагенти” е оторизиран и е възможен само за членовете на Съвета на настоятелите и тези служители на Фондацията, за които това е необходимо за изпълнение на служебните им задължения.

**Чл. 22.** Копирането на документи на хартиен носител или използването на записващи устройства, които позволяват копирането на документи на електронен носител, е позволено само за целите на изпълнение на задълженията на членовете на

Съвета на настоятелите и на служителите на Фондацията, като например изпращане на данни към административни и контролни органи посредством електронен подпис.

**Чл. 23.** Фондацията прилага същите правила на работа в случай на постъпили молби от контрагенти във връзка с упражняване на правата им съгласно ОРЗД.

### **Регистър „Служители”**

**Чл. 24.** Фондацията води отчетност за физически лица, намиращи се в трудови, приравнени на трудови и граждански правоотношения с Фондацията, бивши служители, както и кандидати за работа. За тази цел Фондацията създава и поддържа Регистър „Служители”.

**Чл. 25.** Личните данни на всички служители на Фондацията се обработват на основание Кодекса на труда, Кодекса на социалното осигуряване и приложимите подзаконовни нормативни актове. Данните се въвеждат в специализиран софтуер и съдържат:

1. три имена, ЕГН, постоянен адрес, телефон, имейл;
2. образование, специалност, място на придобиване на образованието, научна степен (ако е приложимо);
3. трудов стаж, сектори, в които лицето е работило, допълнителна квалификация;
4. болнични листове – номер на болничен лист; име на служител; адрес; причина за временната нетрудоспособност; срок на болничния лист, данни на издалия го медицински орган;
5. други документи и информация съгласно приложимото законодателство.

**Чл. 26.** Събраните лични данни се използват за следните цели:

1. индивидуализиране и сключване на трудови и граждански правоотношения;
2. изпълнение на нормативните изисквания на Кодекса на труда, Кодекса за социално осигуряване, Закона за счетоводството, Закона за данъците върху доходите на физическите лица и др.;
3. използване на събраните данни за служебни цели, свързани със съществуването, изменението и прекратяването на трудовите и гражданските правоотношения, воденето на счетоводна отчетност относно възнагражденията на посочените по-горе лица и др.

### **Работа и достъп до лични данни от регистър „Служители”**

**Чл. 27.** Личните данни от Регистър „Служители” се събират, обработват и съхраняват от Съвета на настоятелите и счетоводителя на Фондацията на хартиен

и/или електронен носител, като за всеки служител по трудово правоотношение се съставя и води трудово досие.

**Чл. 28.** Данните за лицата, наети по граждански договори, се събират, обработват и съхраняват от Съвета на настоятелите и счетоводителя на Фондацията на хартиен и електронен носител.

### **ГЛАВА III. ПРАВА НА СУБЕКТИТЕ НА ЛИЧНИ ДАННИ ВЪВ ВРЪЗКА С ОБРАБОТВАНИТЕ ОТ ФОНДАЦИЯТА ЛИЧНИ ДАННИ**

**Чл. 29.** (1) С настоящите правила Фондацията информира своите членове, служители, контрагенти, доставчици, участниците в събития и лицата, използващи услугите на Фондацията, както и всички трети лица, чиито лични данни Фондацията може да събира и обработва, независимо от основанията за това, за правата им във връзка с обработваните лични данни, както следва:

1. право на достъп и информация за обработваните лични данни, както и информация какви лични данни и за каква цел се обработват, кои са получателите на данни, както и какъв е срокът на обработване;
2. право на коригиране на личните данни, които са неточни/неактуални;
3. право на ограничаване обработването на лични данни, в случай че:
  - а) личните данни не са точни, като в този случай ограничаването е за срок, необходим на Фондацията да провери точността;
  - б) обработването на личните данни е неправомерно, но субектът на личните данни не желае те да бъдат изтрети, а само да бъде ограничено използването им;
  - в) Фондацията не се нуждае повече от личните данни за целите на обработването, но субектът на данни ги изисква за установяването, упражняването или защитата на правни претенции;
  - г) субектът на лични данни е възразил срещу обработването в очакване на проверка дали законните основания на Фондацията имат преимущество пред интересите на субекта на данни;
4. право на изтриване – всеки субект, чиито лични данни се обработват от Фондацията по силата на предоставено от него съгласие, може да поиска Фондацията да заличи личните му данни от всички системи и записи, където те се съхраняват, включително да уведоми всички трети лица/обработващи лични данни, на които е предоставила данните, освен ако Фондацията има задължения по закон да съхранява личните данни за определен период от време. Това искане ще бъде удовлетворено, при условие че Фондацията няма правно основание или задължение да съхранява тези данни, и ще бъде под условие на всички срокове, които Фондацията е задължена да спазва в съответствие с приложимите закони и подзаконовни нормативни актове;

5. право на възражение срещу обработването на лични данни. Фондацията следва да се мотивира дали приема искането, респ. защо продължава да обработва личните данни, ако отхвърли искането;

6. право на преносимост на данни – всеки субект на лични данни има право да поиска личните му данни да бъдат предадени в организиран, широко използван и пригоден за машинно четене формат на друго лице (администратор на лични данни), когато това е технически възможно;

7. право на жалба пред Съвета на настоятелите, както и пред компетентния надзорен орган.

(2) Когато има риск за нарушение сигурността на личните данни, Фондацията е задължена да уведоми субектите на лични данни за естеството на нарушението и какви мерки са предприети за отстраняването му, както и дали е уведомен надзорният орган за нарушението.

(3) Всеки субект на лични данни има право на защита по съдебен или административен ред, в случай че правата му във връзка с личните данни са били нарушени.

(4) За да упражни което и да е от правата, изброени по-горе, или при въпроси, свързани с лични данни, всеки субект на лични данни следва да опише искането си в писмен вид и да го адресира по имейл на следния електронен адрес: [baba.bg.association@gmail.com](mailto:baba.bg.association@gmail.com).

(5) Искането трябва да съдържа:

1. име, ЕГН (или друг регистрационен номер, ако е приложим) и адрес на заявителя;
2. описание на искането;
3. предпочитана форма за предоставяне на достъпа до личните данни;
4. подпис, дата на подаване на заявлението и адрес за кореспонденция.

(6) Фондацията разглежда заявлението за достъп и се произнася по него в 30-дневен срок от получаването на искането.

#### **ГЛАВА IV. ДЛЪЖНОСТИ, СВЪРЗАНИ С ОБРАБОТВАНЕТО И ЗАЩИТАТА НА ЛИЧНИ ДАННИ. ПРАВА И ЗАДЪЛЖЕНИЯ**

**Чл. 30.** Съветът на настоятелите отговаря за защитата на личните данни и за спазването на настоящите правила.

**Чл. 31.** При изпълнение на задълженията си Съветът на настоятелите се ръководи от разпоредбите на приложимото законодателство относно защитата на лични данни, както и от настоящите правила.

**Чл. 32.** Съветът на настоятелите има следните задължения:

1. осигурява организацията по воденето на регистрите съгласно предвидените мерки за гарантиране на адекватна защита;

2. упражнява непосредствен контрол върху служителите на Фондацията за спазване на изискванията за защита на личните данни;
3. следи за изправността и правилното функциониране на техническите и програмно-информационните ресурси;
4. следи за опитите и предотвратява такива за неразрешен достъп до базите с данни в регистрите;
5. уведомява лицата, представляващи Фондацията, за всеки опит за неразрешен достъп до системите за сигурност, съответно за осъществен пробив в системите за сигурност, за нанесените щети /ако има такива/ и за предприетите мерки за отстраняване на проблема;
6. ежегодно провежда прегледи относно необходимостта от обработване на данните, както и за заличаването им - за резултатите от извършени проверки се съставя протокол.

**Чл. 33.** Съветът на настоятелите има следните права:

1. право на достъп до обработваната и съхранявана информация от регистрите;
2. право да изисква съдействие от всички служители на Фондацията при изпълнение на служебните им задължения.

## **ГЛАВА V. ТЕХНИЧЕСКИ И ОРГАНИЗАЦИОННИ МЕРКИ ЗА ОСИГУРЯВАНЕ НА НЕОБХОДИМОТО НИВО НА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ**

**Чл. 34.** Личните данни от регистър “Членове на Фондацията”, регистър “Участници в събития и лица, ползващи услугите на Фондацията”, регистър „Служители”, Регистър „Контрагенти” и регистър „Доставчици” (ако е приложимо) се въвеждат в базата данни на Фондацията със защитен достъп.

**Чл. 35.** Във Фондацията са определени различни нива на достъп до лични данни, съхранявани на електронен или хартиен носител, в зависимост от принадлежността към Съвета на настоятелите и длъжностната характеристика на всеки служител на Фондацията и естеството на неговите служебни задължения.

**Чл. 36.** (1) След направен подробен анализ на обработването на лични данни и оценката на въздействието върху защитата на лични данни, Фондацията определя високо ниво на въздействие за регистър “Членове на Фондацията” и регистър “Участници в събития и лица, ползващи услугите на Фондацията”, ниско ниво на въздействие за останалите поддържани регистри и високо ниво на защита на личните данни, обработвани във Фондацията.

(2) Фондацията оценява нивото на въздействие за всеки поддържан регистър, както следва:

	Ниво на въздействие	Поверителност	Цялостност	Наличност	Общо за регистъра
Регистър "Членове на Фондацията"	високо	високо	високо	високо	високо
Регистър "Участници в събития и лица, ползващи услугите на Фондацията"	високо	високо	високо	високо	високо
Регистър „Служители“	Ниско	Ниско	Ниско	Ниско	Ниско
Регистър „Контрагенти“	Ниско	Ниско	Ниско	Ниско	Ниско
Регистър „Доставчици“	Ниско	Ниско	Ниско	Ниско	Ниско

**Чл. 37.** Съгласно настоящите правила видовете защита и нейните нива са следните:

1. автоматизирани информационни системи и/или мрежи, включващи следното:

а) непосредствен достъп до локалната мрежа имат само Съветът на настоятелите и определени служители на Фондацията чрез двуфакторна автентикация. Служителите имат достъп само до данни и ресурси, необходими за изпълнение на служебните им задължения;

б) за осигуряване надеждност и интегритет на компютърната система, Фондацията прилага различни практики включително, но не само, сигурна конфигурация на устройствата, редовни външни и вътрешни проверки за уязвимости, регулярно обновяване, филтриране на входящия и изходящия трафик, резервно хранване, отделяне на сървъри в специално помещение, периодични копия и други.

2. осъществяване на редовна профилактика на компютрите и комуникационните средства, включващо:

а) профилактика на компютрите и проверка за вируси, шпионски софтуер, проверка на твърди дискове за грешки, дефрагментация на твърди дискове, актуализация на операционната система и използвания софтуер;

б) за предпазване на компютърната мрежа от неправилен достъп през интернет се използва специализирано устройство – защитна стена (Firewall), което следи и филтрира входящия и изходящия трафик, премахвайки автоматично зловреден код и блокирайки всички връзки, освен изрично разрешените;

в) профилактика на компютрите и комуникационните средства, която се извършва от системните администратори ежедневно, на място в офиса на Фондацията и чрез отдалечен достъп, когато е необходимо;

г) при идентифициране на инциденти за резултата от проверката се уведомяват лицата, представляващи Фондацията.

д) IT профилактиката и техническата поддръжка на IT системите във Фондацията се извършва изцяло от служители на Фондацията, без да се ползват външни контрагенти.

3. физическа защита (определяне на зоните с контролиран достъп и на използваните технически средства за физическа защита): офисът на Фондацията, в който са поставени компютрите, се заключва и се достъпва от членовете на Съвета на настоятелите и съответните служители, които работят в съответното помещение и разполагат с копие от ключа. Помещенията, в които има компютри, които поддържат офисната мрежа на Фондацията, са снабдени със сигнално-охранителна система с цел осигуряване по-висока степен на защита на съхраняваните данни.

4. персонална защита:

а) офисът на Фондацията е в пълно съответствие с нормативните изисквания за пожарна безопасност и е снабден със специални средства за защита от пожар. Съветът на настоятелите следи за спазването на мерките за безопасност;

б) всеки служител е длъжен да споделя констатирана от него критична информация. Всеки служител, отговорен за обработването на лични данни и/или имащ достъп до тях, е длъжен да познава и прилага правилата за защита на личните данни.

5. документална защита:

а) непосредствен достъп до данните на хартиен носител от регистър „Служители” имат само определени служители, включително счетоводителят на Фондацията, който извършва превод на работните заплати, както и Съветът на настоятелите на Фондацията.

б) достъп до регистър „Доставчици” и регистър „Контрагенти” имат членовете на Съвета на настоятелите и служителите, на които данните от съответния регистър са необходими за изпълнение на служебните им задължения, включително Съветът на настоятелите и счетоводителят на Фондацията. Личните данни, съхранявани на хартиен носител, са разположени в обособени помещения и заключващи се шкафове, достъп до които имат само оторизираните за това служители.

в) достъп до регистър “Членове на Фондацията” и регистър “Участници в събития и лица, ползващи услугите на Фондацията” имат членовете на Съвета на настоятелите и служителите, на които данните от съответния регистър са необходими за изпълнение на служебните им задължения, включително Съветът на настоятелите. Личните данни, съхранявани на хартиен носител, са разположени в обособени помещения и заключващи се шкафове, достъп до които имат само оторизираните за това служители.

6. псевдонимизация и криптографска защита:

а) Фондацията въвежда, както към момента на определянето на средствата за обработване, така и към момента на самото обработване, подходящи

технически и организационни мерки, които са разработени с оглед на ефективното прилагане на принципите за защита на данните, които включват, наред с другото, псевдонимизация, свеждане на данните до минимум, както и интегриране на необходимите гаранции в процеса на обработване, за да се спазват изискванията на ОРЗД и да се осигури защита на правата на субектите на данни;

б) Фондацията въвежда псевдонимизация на личните данни на етап проектиране и по подразбиране. Фондацията счита, че прилагането на псевдонимизация на личните данни може да намали съществено рисковете за съответните субекти на данни и да помогне на Фондацията да изпълнява своите задължения за защита на данните;

в) в допълнение, Фондацията използва криптографските възможности на операционните системи за управление на бази данни и стандартните криптографски възможности на комуникационното оборудване.

**Чл. 38.** Счетоводителят на Фондацията, когато е външно лице, както и други външни консултанти на Фондацията, предприемат мерки на защита, еквивалентни на мерките съгласно тази глава.

## **ГЛАВА VI. ДЕЙСТВИЯ ЗА ЗАЩИТА ПРИ АВАРИИ, ПРОИЗШЕСТВИЯ И БЕДСТВИЯ**

**Чл. 39.** (1) Всеки служител на Фондацията е длъжен да уведоми незабавно Съвета на настоятелите при възникване на авария, произшествие и бедствие, при който е или би могла да бъде засегната сигурността на съхраняваните лични данни в базата данни на Фондацията.

(2) Непосредствено след като е уведомено за настъпването на инцидент по Съветът на настоятелите следва да предприемат всички необходими действия за потвърждаване на валидността на уведомлението, ограничаване на щетите и бъдещо предотвратяване, в т.ч. да уведомят лицата, представляващи Фондацията.

(3) При първа възможност Съветът на настоятелите уведомява представляващите Фондацията лица за събитието по ал. 1, като ги информира за:

1. описание на инцидента;
2. времето на установяването на инцидента;
3. лицето, което докладва за инцидента;
4. последствията от инцидента и мерките за отстраняването му.

(4) В случай на нарушение на сигурността на личните данни Съветът на настоятелите без ненужно забавяне и когато това е осъществимо — не по-късно от 72 часа след като е го е потвърдил, уведомява за нарушението на сигурността на личните данни компетентния надзорен орган, а именно Комисията по защита на личните данни. Уведомлението до надзорния орган съдържа причините за забавянето, когато не е подадено в срок от 72 часа.

(5) В уведомлението до компетентния надзорен орган съгласно предходния член се съдържа най-малко следното:

1. описание на естеството на нарушението на сигурността на личните данни, включително, ако е възможно, категориите и приблизителният брой на засегнатите субекти на данни и категориите и приблизителното количество на засегнатите записи на лични данни;
2. посочване на името и координатите за връзка на Съвета на настоятелите, от който може да се получи повече информация;
3. описание на евентуалните последици от нарушението на сигурността на личните данни;
4. описание на предприетите от Фондацията мерки за справяне с нарушението на сигурността на личните данни, включително мерките за намаляване на евентуалните неблагоприятни последици.

(б) Фондацията документира всяко реално нарушение на сигурността на личните данни, включително фактите, свързани с нарушението на сигурността на личните данни, последиците от него и предприетите действия за справяне с него.

## **ГЛАВА VII. СЪОБЩАВАНЕ НА СУБЕКТА НА ДАННИТЕ ЗА НАРУШЕНИЕ НА СИГУРНОСТТА НА ЛИЧНИТЕ ДАНИ**

**Чл. 40.** (1) Когато има вероятност нарушението на сигурността на личните данни да породи висок риск за правата и свободите на физическите лица, Фондацията, без ненужно забавяне, съобщава на субекта на данните за нарушението на сигурността на личните данни.

(2) В съобщението до субекта на данните, на ясен и точен език се описва естеството на нарушението на сигурността на личните данни и се посочват най-малко информацията, която е съобщена на компетентния надзорен орган.

(3) Съобщение до субекта на данните не се изисква, ако някое от следните условия е изпълнено:

1. Фондацията е предприела подходящи технически и организационни мерки за защита и тези мерки са били приложени по отношение на личните данни, засегнати от нарушението на сигурността на личните данни, по-специално мерките, които правят личните данни неразбираеми за всяко лице, което няма разрешение за достъп до тях, като например криптиране;
2. Фондацията е взела мерки, които гарантират, че вече няма вероятност да се материализира високият риск за правата и свободите на субектите на данни;
3. подобно съобщение би довело до непропорционални усилия. В такъв случай се прави публично съобщение или се взема друга подобна мярка, така че субектите на данни да бъдат в еднаква степен ефективно информирани.

## **ГЛАВА VIII. СЪХРАНЯВАНЕ, АРХИВИРАНЕ И УНИЩОЖАВАНЕ НА ЛИЧНИ ДАНИ**

**Чл. 41.** Личните данни се съхраняват в заключващи се шкафове в помещенията на Фондацията и нейния счетоводител, както и на сървъри в нейната мрежа.

**Чл. 42.** Фондацията съхранява личните данни в регистър “Членове на Фондацията” през времетраенето на членството им, освен ако по силата на закон или акт на компетентен орган или за целите на защитата на законните права и интереси на Фондацията се изисква по-дълъг срок.

**Чл. 43.** Фондацията съхранява личните данни в регистър “Участници в събития и лица, ползващи услугите на Фондацията” в продължение на до 6 месеца, освен ако по силата на закон или акт на компетентен орган или за целите на защитата на законните права и интереси на Фондацията се изисква по-дълъг срок.

**Чл. 44.** Счетоводителят на Фондацията съхранява личните данните в регистър „Контрагенти” в продължение на целия период на съществуване на договорните отношения със съответния контрагент, но не по-малко от 5 години след прекратяване на договорните отношения с контрагента, независимо от причините за прекратяването.

**Чл. 45.** (1) Счетоводителят на Фондацията съхранява следните лични данни от регистър „Служители“ за срок не по-дълъг от 50 (петдесет) години от възникването на трудовото правоотношение: трудов договор, длъжностна характеристика, ведомости за заплати. Отделни лични данни от регистър „Служители“ се съхраняват за по-кратък срок, като например болнични листове, които се съхраняват за срок от 3 (три) години, считано от началната дата на издаване на болничния лист. Личните данни по настоящия член се съхраняват на хартиен и електронен носител.

(2) Съветът на настоятелите отговаря за правилното съхраняване на личните данни в съответните регистри. Унищожаването на лични данни може да бъде извършвано само от определени служители след изрично указание на Съвета на настоятелите, в което са указани видовете лични данни, срокът и начинът на унищожаване.

**Чл. 46.** В допълнение, след изтичане на гореспоменатите срокове за съхранение, Съветът на настоятелите издава указания за унищожаването на съответните лични данни, чрез които възлага на определен служител тяхното унищожаване, както следва:

1. лични данни, съхранявани на хартиен носител – машинно унищожаване чрез шредер;
2. лични данни, съхранявани на електронен носител – изтриване от електронната база данни/ сървъри.

## **ГЛАВА IX. ПРЕДОСТАВЯНЕ НА ЛИЧНИ ДАННИ НА ТРЕТИ ЛИЦА И УПРАЖНЯВАНЕ ПРАВАТА НА СУБЕКТИТЕ НА ЛИЧНИ ДАННИ**

**Чл. 47.** Фондацията има право да разкрива информация относно съхраняваните лични данни само:

1. на субекта на данни или на изрично упълномощено от него лице, което предоставя нотариално заверено пълномощно с представителна власт, при спазване на процедурите за достъп до личните данни;
2. на свои контрагенти, когато обработването е необходимо за изпълнението на договор между Фондацията и контрагента, при спазване на законодателството за защита на личните данни;
3. на компетентните държавни органи в определените от закона случаи и по определения от закона ред.

## **ГЛАВА X. ОБУЧЕНИЕ НА СЛУЖИТЕЛИТЕ**

**Чл. 48.** (1) При постъпване на работа във Фондацията, Съветът на настоятелите запознава всеки служител с настоящите правила и нормативните документи, свързани с мерките за защита на личните данни, което се удостоверява с подписването на декларация.

(2) Съветът на настоятелите периодично информира служителите на Фондацията за настъпили промени в начина на защита на личните данни, включително за промени в настоящите правила и/или за промени в нормативната уредба. За всеки проведен инструктаж по предходното изречение се изготвя и подписва протокол.

(3) Всички новопостъпили служители на работа във Фондацията след 12.09.2025 г. преминават индивидуално онлайн обучение и тест, което обучение го запознава с изискванията на ОРЗД в срок от 3 (три) работни дни след постъпването им на работа.

## **ГЛАВА XI. ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ**

**§ 1.** Настоящите Правила се приемат на основание ОРЗД, ЗЗЛД и останалите подзаконови нормативни актове на Република България.

**§ 2.** Жалби за нарушения на настоящите правила могат да се подават пред Съвета на настоятелите на Фондацията, адрес: гр. София, п.к. 1000, район "Триадица", ул. "Кърниградска" № 19, ет. 1, ел. адрес: [baba.bg.association@gmail.com](mailto:baba.bg.association@gmail.com), както и пред Комисията за защита на личните данни, адрес: гр. София 1592, бул. „Проф. Цветан Лазаров” № 2; ел. адрес: [kzld@cpdp.bg](mailto:kzld@cpdp.bg); уеб сайт: [www.cpdp.bg](http://www.cpdp.bg).

Настоящите Правила са приети с решение на Съвета на настоятелите на 12.09.2025 г. и влизат в сила от същата дата.