BG

ПОЛИТИКА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

на сдружение с нестопанска цел в частна полза

“ СДРУЖЕНИЕ НА ФАМИЛНИЯ БИЗНЕС- БЪЛГАРИЯ“

ASSOCIATION OF THE FAMILY BUSINESS - BULGARIA

(FBN-BULGARIA)

Утвърдена с Заповед № … / … на Председателя на Управителния съвет на “Сдружение на фамилния бизнес-България”

25 май 2018 година

Съдържание

Въведение

(1) Считано от 25 май 2018 година влиза в сила 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 и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО ***(по-долу GDPR)****. GDPR се прилага непосредствено за всяко обработване на лични данни от страна на администратор или обработващ, установени на територията на Европейския съюз.*

(2) Като организация, установена на територията на Република България и обработваща лични данни на български граждани, граждани на други държави членки на ЕС, както и на граждани на трети страни, представляващи организации от семейството на Family Business Network International и European Family Business, за сдружение с нестопанска цел в частна полза ***"Сдружение на фамилния бизнес - България"****, регистрирано по фирмено дело 16408 по описа на Софийски градски съд за 2006 година, в Регистъра на юридическите лица с нестапска цел с* ***ЕИК: 175207708****, със седалище и адрес на управление в гр. София, п.к. 1124, р-н Средец, бул. "Цариградско шосе", Полиграфия офис център №47А, ет. 3****,*** *представлявано от председателя на Управителния съвет адвокат Стефан Марков Гугушев* ***(по-долу "Сдружението" или "FBN-Bulgaria")*** *възникват редица задължения в съответствие с Регламент 2016/679/ЕС, Насоките на Работната група по член 29 от Директива 95/46/ЕО, и останалите актове на приложимото европейско и вътрешно право (*"***Приложимото право относно защита на данните")****.*

*(3) С оглед на необходимостта от осигуряването на подходящи технически и организационни мерки за гарантиране на законосъобразността и прозрачността на извършваното от Сдружението обработване на лични данни при реализиране на дейността му по подпомагане на семействата в България в бизнеса им и популяризиране на техните успехи, Сдружението утвърждава и приема да се придържа към настоящата Политика за защита на личните данни **("Политиката")**, която, ведно с посочените по-долу приложения към нея, както и останалите правила, процедури, стандарти и оценки на въздействието, урежда защитата на обработваните данни и отчетността за Сдружението.*

Дефиниции

Всички термини, използвани в Политиката, се ползват и тълкуват със значението, с което са употребени в GDPR и останалите актове на Приложимото право относно защитата на данните, освен ако по-долу не е посочено друго:

- **"Лични/те данни"** означава всяка информация, свързана със Субектите на данни, включително име, подпис, фото- или видеообраз, ЕГН, номер на документ за самоличност, дата на издаване/валидност на документа или копие от същия, дата на раждане, постоянен или настоящ адрес, IP адрес, или други признаци, специфични за физическата, физиологичната, генетичната, психическата, умствената, икономическата, културната или социална идентичност на тези лица.

- **"Специални категории лични данни"** означава Лични данни, разкриващи расов или етнически произход, политически възгледи, религиозни или философски убеждения, членство в синдикални организации, както и обработването на генетични или биометрични данни за целите единствено на идентифицирането на физическо лице, данни за здравословното състояние или данни за сексуалния живот или сексуалната ориентация на Субектите на данни.

- "**Администратор/ът на лични данни"** или **"Администратор/ът"** означава Сдружението в случаите, в които съответната дейност, по отношение на която се явява администратор, се извършва от името и за сметка на Сдружението, в негова полза или с неговите средства (уебсайт, профил в социална мрежа). Всички дейности по обработване, по отношение на които Сдружението се явява администратор, ще бъдат отразени в съответния регистър.

- **“Обработващ/ият лични данни”** или **“Обработващ/ият”** означава: (1) Сдружението, в случаите, в които осъществява съответната дейност от чуждо име и за чужда сметка, в чужда полза или с чужди средства (напр. платформа и/или уебсайт, профил в социалните мрежи, канал в YouTube и т.н.), както и (2) всяко лице, различно от Сдружението и неговите членове и служители, което обработва Данните от името и за сметка на Сдружението, в негова полза или с неговите средства. Обработващи по-специално са контрахентите, с които Сдружението обменя данни при реализиране и популяризиране на дейността си и с които сключва споразуменията по член 28, параграф 3 от GDPR. Дейностите по обработване, по отношение на които Сдружението се явява обработващ, ще бъдат отразени в съответния регистър.

- **“Субект на данни”** означава всяко физическо лице, за което се отнасят Личните данни. По смисъла на настоящата политиката субекти на данни са по-специално бившите и настоящи служители на Сдружението, кандидатите за работа, физическите лица, представляващи бившите и настоящи членове на Сдружението , представляващите кандидатстващите за членство в Сдружението организации, както и всички останали физически лица, чиито лични данни се обработват от Сдружението.

- **“Обработване”** означава всяка дейност или съвкупност от дейности, извършвани с Личните данни, включително публикуване на Данните на сайта на Сдружението и в профилите му в социалните мрежи, както и техния обмен в рамките на FBN International и чрез платформата FBN Xchange. Пълен списък на членовете на семейството на FBN International може да бъде намерен тук.

- **“Заявление за упражняване на права”** или **“Заявление”** означава всяко писмено искане, отправено от Субект на данни до Сдружението чрез ел. поща или уебсайта на Сдружението, във връзка с обработването на неговите Данни и засягащо упражняване на едно или няколко права, предвидени в GDPR. Заявленията за упражняване на права се разглеждат по реда, предвиден в Процедурата за разглеждане на заявленията на субектите на данни **(Приложение №5 към Политиката)**.

- **“Съгласие”** означава свободно изразено, конкретно, информирано и недвусмислено указание за волята на Субектите на данни. Сдружението обработва Данните на Субектите въз основа на тяхното съгласие единствено при осъществяването на активности, целящи популяризиране на дейността на Сдружението и неговите членове, включително публикации на сайта и страниците му в социалните мрежи, изготвяне и разпространение на ежемесечния имейл бюлетин. Информацията относно съгласията за обработването на Данните се води в нарочен регистър, воден от Сдружението.

- **“Дете”** означава всеки член на семейство, част от Сдружението, който не е навършил 16-годишна или друга, по-ниска възраст ако такава бъде определена в Приложимото право относно защита на данните. Данни на деца се обработват от Сдружението само и единствено със знанието и разрешението на родителя/настойника.

- **“Отговорник/ът относно защитата на данните”** означава определено с акт на председателя на Управителния съвет лице, на което са възложени дейностите, свързани със спазването и осигуряване на отчетност за спазването на Приложимото право относно защита на данните.

- **“Служители на Сдружението”** или само **“Служители”** по-долу означава всички лица, изпълняващи трудова дейност в съответствие със сключен трудов или граждански договор, която дейност включва обработване на Личните данни.

- **“Надзорен орган”** означава Комисията за защита на личните данни на Република България (КЗЛД) или друг орган, определен в съответствие с Приложимото право относно защита на данните.

- **“Трета страна”** или **“Трети страни”** означава физическо или юридическо лице, публичен орган, агенция или друга организация, различна от споменатите по-горе.

Декларации

(1) Сдружението декларира, че при осъществяване на дейността си се ангажира да спазва всички правни актове на ЕС и Република България относно защитата на данните, както и да защитава и способства упражняването на правата на Субектите, чиито данни събира и обработва.

(2) Сдружението декларира, че предвижда механизми за правно съответствие и гарантиране на спазването на GDPR чрез настоящаща политика, ведно с приложенията към нея, по отношение на всички дейности, свързани с обработването на Личните данни.

(3) Сдружението декларира, че Младежката структура "Следващото поколение" (**FBN-NextGen**) представлява единна и неделима част от него, по отношение на която на абсолютно основание се прилагат всички механизми и ангажименти, свързани с обработване и защита на Личните данни, посочени в настоящата политика.

(4) Сдружението декларира, че прилага Политиката по отношение на всички свои служители, представители, членове и техните семейства, партньори и всякакви други лица, обработващи Данните като например системни администратори, PR компании, медии, доставчици и счетоводни кантори. **Всяко нарушение на Политиката и приложенията към нея ще бъде разглеждано съгласно дисциплинарната политика на Сдружението.**

(5) Сдружението декларира, че си сътрудничи единствено с партньори и Трети страни, задължили се да спазват правила, гарантиращи ниво на защита на Данните, минимум съответстващо на предвиденото от настоящата политика. Освен ако Приложимото право относно защитата на данните не предвижда друго, на Обработващи, които предварително не са сключили споразуменията по GDPR, няма да бъде даден достъп до Данните.

(6) Сдружението декларира, че си запазва правото по всяко време да следи за спазването от страна на своите партньори на задълженията, свързани със защитата на Личните данни, включително като пряко или чрез специализирано лице-одитор организира всякакви проверки и одити за спазване на Приложимото право относно защитата на данните и настоящага политика.

Принципи за защита на данните

Сдружението обработва Личните данни в съответствие с принципите, свързани със защита на данните, посочени в член 5 от GDPR. Политиката гарантира спазването на тези принципи:

Личните данни се обработват:
законосъобразно, добросъвестно и прозрачно

- *Законосъобразно:*

  Данните се обработват само при валидно правно основание.

- *Добросъвестно:*

  Сдружението предоставя на Субектите цялата информация, свързана с обработването и защитата на техните данни, доколкото е практически възможно, независимо дали Данните са получени пряко от Субекта или от други източници.

- *Прозрачно:*

  В съответствие с принципа на прозрачно обработване на Личните данни, Сдружението предоставя информацията, свързана с обработването и защитата на Данните на Субектите в разбираема и достъпна форма на ясен и прост език като **уведомление относно обработването на лични данни (privacy notice)**. Те включват най-малко:

  - информация, която идентифицира Сдружението и неговите представители;
  - данни за контакт по въпросите, свързани със защитата и обработването на Личните данни на Субектите;
  - целите и правното основание за обработването;
  - сроковете за съхранение на обработваните данни;
  - правата на Субектите на дани, както и условията, свързани с упражняването на тези права;
  - категориите обработвани данни;
  - възможните категории получатели на Данните;
  - друга допълнителна информация за обработването.

Личните данни могат да бъдат събирани единствено за конкретни, изрично указани и легитимни цели.

Личните данни трябва да бъдат подходящи, свързани с и ограничени до необходимото за обработването.

Личните данни трябва да бъдат точни и актуални, своевременното изтривани или коригирани.

Данните, съхранявани от Сдружението, трябва да бъдат преглеждани и актуализирани, когато е необходимо. Не се съхраняват данни за които не може основателно да се приеме, че са точни. **Формулярите за събиране на данни включват декларация, че предоставените данни са точни и актуални.**

Личните данни се съхраняват във формат, позволяващ идентифициране на Субектите, и не по-дълго от необходимото.

Личните данни се съхраняват за сроковете, посочените в Политиката за съхранение, блокиране и заличаване, след изтичането на които се унищожават по сигурен начин. Ако има причина Данните да продължат да се съхраняват след изтичането на съответния срок, те се анонимизират, псевдономизират и/или свеждат до минимум с цел запазване самоличността на Субектите при нарушение на сигурността.

Личните данни трябва да бъдат обработвани по начин, гарантиращ подходящо ниво на сигурност.

При определяне на организационни мерки, осигуряващи подходящото ниво на сигурност на Данните Сдружението взе предвид степента на евентуалните вреди, които могат да бъдат причинени на субектите на данните при нарушение в сигурността, и всички последици от нарушението, включително накърняване на репутацията на лицата.

Сдружението определи следните организационни мерки за защита на данните:

- обучаване на служителите относно защитата на Данните;
- включване в трудовите и гражданските договори на правила, свързани с обработването и защитата на Данните;
- контрол за спазване на правилата за защитата на Данните;
- прилагане на Политика за чисти работни места;
- ограничаване на достъпа до Данните извън работното място;
- въвеждане на правила за паролите, позволяващи индивидуална идентификация на служителите;
- въвеждане на органичен достъп до Данните на база "Необходимост да знае".

Личните данни трябва да бъдат обработвани по начин, позволяващ документирането на спазването на Приложимото право относно защитата на данните ("отчетност"). В тази връзка Сдружението приема всички необходими мерки включително, но не само, изготвяне на документи в писмена, включително електронна, форма, утвърждаване на образци на регистри, както и на бланки за комуникация с Надзорния орган, администраторите и обработващите, и със субектите на данни.

Права на субектите на данни

В съответствие с GDPR Субектите имат следните права:

- да получават информация относно обработването на Данните им и на кого те са били или могат да бъдат разкрити, включително да получат копие от документите, съдържащи техните данни в структуриран, широкоизползван и пригоден за машинно четене формат;

- да възразят срещу дейностите по обработване на Личните им данни, които могат да им причинят вреди;

- да оттеглят по всяко време даденото от тях съгласие за обработване на Личните им данни и/или да поискат временно преустановяване ("блокиране") на обработването;

- да търсят обезщетение за действително претърпените вреди поради нарушение от страна на Сдружението на Приложимото право относно защита на данните и Политиката и приложенията към нея;

- да предприемат действия за коригиране, блокиране, изтриване или унищожаване на неточни данни;

- да получат информация как могат да сигнализират Надзорния орган по всяко време, независимо от предвиденото в Политиката и приложенията към нея.

Сдружението способства упражняването на правата на Субектите на данните по реда, предвиден в Процедурата за разглеждане на заявления за упражняване на права на субектите на данни (Приложение №5 към Политиката).

Отговорности и роли на служителите съгласно GDPR

1. Всички лица, които изпълняват управленски или надзорни роли, са отговорни за разработването и насърчаването на добри практики за обработване на Данните.

2. Спазването на законодателството за защита на данните е отговорност на всички служители, обработващи Данните.

3. Служителите на Сдружението гарантират, че всички Лични данни, свързани с тях и/или предоставени от тях на Сдружението, са точни и актуални.

Отговорник относно защитата на данните

1. Отговорникът относно защитата на данните се определя по реда на утвърждаване на настоящата политика със заповед на Председателя на Управителния съвет на Сдружението.

2. Директорът на Сдружението може да бъде избран да изпълнява функциите на Отговорник относно защитата на данните. В този случай контролът относно спазването на Политиката от страна на Директора се осъществява от Председателя на Управителния съвет.

3. Отговорникът по защитата на данните:

   - осъществява контрол за спазването на Приложимото право относно защита на данните, включително преглед за съответствието на Политиката и приложенията към нея с Приложимото право относно защита на данните **поне веднъж на всеки две години**;

   - осъществява сътрудничество с Надзорния орган, включително предварителна консултация и уведомяване при нарушение в сигурността на Данните в предвидените от Приложимото право относно защитата на данните случаи;

   - осъществява сътрудничество със Субектите на данните, включително при предявяване на заявление за упражняване на правата им, разглеждане на заявленията и съобщаване при нарушение в сигурността на Данните;

- В съответствие със Стандарта за извършване на оценка на въздействието на риска върху защитата на Данните (Приложение №2 към Политиката) проверява всеки процес, който предстои да бъде имплементиран, и който включва в себе си обработване на Личните данни в съответствие с принципа за защита на данните на етапа по проектиране и по подразбиране;

- дава становища и препоръки, както и да осъществява сътрудничество от всякакъв друг характер с цел осигуряване спазване и отчетност за спазването на Приложимото право относно защита на данните.

Запазване и унищожаване на данни

1. Сдружението продължава да съхранява Личните данни след изтичане на определения срок за съхранение единствено за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели само ако бъдат приложени подходящи мерки за защита на правата на Субектите на данните.

2. Сроковете за съхранение за различните категории Данни, респективно документи, в които Данните се съдържат, са посочени в Политиката за съхранение, блокиране и заличаване на Данните. Всяко унищожаване на Данни се извършва в съответствие с Приложимото право относно защитата на данните, Политиката и Политиката за съхранение, блокиране и заличаване на Данните.

Разкриване на данни пред трети страни

1. Служителите осигуряват условия Данните, обработвани в рамките на процесите, за които носят отговорност, да се съхраняват по сигурен начин и да не се оповестяват на Трети страни при никакви условия, освен ако не са упълномощени и не са сключили споразумение по GDPR или ако задължение за разкриване не възниква по силата на Приложимото право относно защитата на данните.

2. Всякакви искания за разкриване на Личните данни трябва да бъдат съпроводени от съответните документи, удостоверяващи правото на Третата страна да получи достъп. Исканията, ведно със съпровождащите ги документи, се преглеждат от Отговорника за защитата на данните, който се произнася с мотивирано решение.

Политика за чисти работни места

1. Всички лични данни трябва да бъдат достъпни само за лицата, които се нуждаят от тях. Всички лични данни трябва да бъдат разглеждани с най-висока степен на сигурност и трябва да бъдат съхранявани:
   - в стая с контролиран достъп, която се заключва, и/или
   - в заключено чекмедже или шкаф, и/или
   - ако са в електронен формат, със защитена парола или на (преносими) електронни носители, които са криптирани.
2. Служителите са длъжни да не оставят документи върху бюрата си или по отворени рафтове в близост до тях, когато не са на работното си място за по-дълго време (над 20 мин.). Конфиденциални документи и документи с чувствителен характер не се оставят без надзор при никакви условия.

3. Всички чекмеджета и шкафове от бюрото на съответния служител трябва да са заключени докато служителят е извън сградата и/или в неработно време.

4. Служителите се задължават винаги да носят със себе си ключовете от кабинетите, чекмеджетата, шкафовете и други поверени им контейнери, в които се съхраняват документи, или да ги държат под ключ.

5. В края на работния ден служителите почистват бюрата си, изключват осветлението и климатиците и заключите вратите на кабинетите, респективно включват алармата на офисните помещения.

Видеонаблюдение

1. Записите от техническите средства, посредством които на територията на помещенията на Сдружението се осъществява видеонаблюдение се съхраняват за сроковете, определени в Политиката за съхранение, блокиране и заличаване на данните. Правно основание за осъществяване на видеонаблюдението е легитимния интерес на Сдружението да осигури сигурността на служителите и имуществото си.

2. Видеонаблюдението се извършва само на изрично означените с уведомление за видеонаблюдение и/или стикери за видеонаблюдение, реферирaщи към уведовлението, места, без по никакъв начин да се засягат правата и достойнството на Субектите на данни (например не се осъществява видеонаблюдение в тоалетните и кухненски помещения).

Технически мерки за защита на информационната и мрежовата инфраструктура за обработване на данни

1. Сдружението гарантира, че предприема адекватни технически мерки за защита на информационната и мрежовата си инфраструктура, необходима за продължаване на дейността в случай на нарушение на сигурността на данните.
2. Мерките за защита на помещенията с мрежовата и информационната инфраструктура на Сдружението включват по-специално:
   (1) мерки за ограничаване на физическия достъп по помещенията, в който се съхраняват документите и сървърите на Сдружението, включително регистриран достъп посредством чип-карти и физическа охрана.
   (2) осъществянане на видеонаблюдение (CCTV);
   (3) използване на служебни имейл акаунти на служителите за комуникация;
   (4) разполагане на сензори и датчици за засичане на опасност от пожар в помещенията на Сдружението;
   (5) наличие на пожарогасители в помещенията на Сдружението;
   (6) запазване на електронно резервно копие от данните на сървъра на Сдружението.

Запазване на електронни резервни копия (back-up)

1. Данните в информационните системи на Сдружението се защитават посредством периодично запазване на електронно копие от същите (back-up) ежедневно и ежемесечно в съответствие с определеното ниво на сигурност и достъп.

2. Ключовите елементи от информационната инфраструктура на Сдружението и активите също се защитават чрез back-up, така че при нарушение в следствие на злоумишлен софтуер Сдружението да продължи дейността си по достъп и обработване на данните.

3. Сдружението гарантира, че сроковете за съхранение на резеврните копия от данните не надвишават определените срокове за съхранение на основните документи.

4. Резервни копия, чието ползване е преустановено, или които са станали нечетими или неизползваеми, се заличават.

Осъществяване на дистанционен достъп

1. За обработване на данни служителите използват наличната техническа и информационна инфраструктура.

2. Председателят на Управителния съвет може да разреши осъществяването на следните форми на дистанционен достъп при отправяне на молба от съответния служител с оглед на изпълнение на служебните му задължения:

   (1) достъп до служебна електронна поща от служебно мобилно електронно устройство;

   (2) достъп до служебна поща от лично мобилно или стационарно електронно устроойство;

   (3) отдалечен (VPN) достъп до службната поща и сървърите на Сдружението.

3. Устройствата, чрез които се осъществява дистанционен достъп до Данните, подлежат на вписване в нарочен регистър.

Списък на приложенията

Приложение №1	Политика за съхранение, блокиране и заличаване на личните данни
Приложение №2	Стандарт за извършване на оценка на въздействието на риска върху защитата на данните
Приложение №3	Процедура за уведомяване на надзорния орган за нарушение на сигурността на личните данни
Приложение №4	Процедура за съобщаване на субектите на данни за нарушение на сигурността на личните данни
Приложение №5	Процедура за разглеждане на заявления за упражняване на права на субектите на данни
Приложение №6	Процедура за обучение на служителите

Списък на ревизиите

Версия 1	Изготвена и приета към 25-ти май 2018-та година в съответствие с Регламент 2016/679/ЕС (Общ регламент относно защитата на данните)