



## ПОЛИТИКА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

### БЪЛГАРСКА АСОЦИАЦИЯ ЗА АЛТЕРНАТИВЕН ТУРИЗЪМ (БААТ)

*като взе предвид* приетия на 27 април 2016 г. **Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27.04.2016 г. 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**, наричан по-нататък “Общ регламент за защита на данните” или “Регламента”

*и в съответствие с факта*, че Регламентът е задължителен в своята цялост и се прилага пряко във всички държави членки на Европейския съюз  
*и в съответствие с* националното законодателство и приетите добри практики в областта на защитата на личните данни

*и като има предвид, че:*

защитата на физическите лица във връзка с обработването на лични данни  
е основно право

Прие настоящата ПОЛИТИКА ЗА ЗАЩИТА НА ЛИЧНИ ДАННИ, с решение на Управителния съвет от 12 април 2018 г., която има за цел да информира физическите лица (членове, клиенти, партньори, доставчици, потребители на сайт и други физически лица) за целите на обработване на личните данни, получателите или категориите получатели, на които могат да бъдат разкрити данните, принципите, които се спазват при обработването на лични данни, както и за реда за упражняване на правата на субектите на лични данни.

### Общи положения

**Българска асоциация за алтернативен туризъм (БААТ)** е сдружение в обществена полза, вписано в Търговския регистър при Агенцията по вписванията с ЕИК 121703113, със седалище и адрес на управление: София, бул. Ал. Стамболийски 20В, наричано по-нататък „Сдружението“.

Сдружението само определя целите и средствата за обработване на лични данни и в този смисъл се явява Администратор на лични данни по смисъла на чл.4, т.7 от Регламента.

При събирането и обработването на лични данни Сдружението спазва закони и нормативни правила, които разпореждат как да бъдат извършвани действията по събиране и обработка на лични данни, както и какви гаранции за защита на личните данни да бъдат приложени. Нормативната уредба включва, но не се ограничава до



Общия регламент за защита на личните данни (Регламент (ЕС) 679/2016), Кодекса на труда, Кодекса за социално осигуряване, Закона за защита на личните данни, Закона за счетоводството, Закона за юридическите лица с нестопанска цел, както и издадените въз основа на тях подзаконовни нормативни актове, Устава на Сдружението.

Сдружението защитава личните данни, като прилага всички подходящи технически и организационни мерки, с които разполага, за да не допуска неразрешен достъп, неразрешено или злонамерено ползване, загуба или преждевременно заличаване на информация.

Тази политика се прилага за всички системи, хора и процеси, които изграждат информационната система на Сдружението, включително спрямо лицата, заемащи управленски длъжности, служителите, доставчиците и всички други трети лица, които имат достъп до системите с лични данни на Сдружението.

### Използвани термини и дефиниции.

По смисъла на настоящата Политика и съгласно Регламента:

1. **„Лични данни“** са всяка информация, свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано („*субект на данни*“);

2. **„Субект на данни“** е физическо лице, което е идентифицирано или може да бъде идентифицирано, пряко или непряко, по-специално чрез идентификатор като име, идентификационен номер, данни за местонахождение, онлайн идентификатор или по един или повече признаци, специфични за физическата, физиологичната, генетичната, психическата, умствената, икономическата, културната или социална идентичност на това физическо лице.

3. **„Обработване“** означава всяка операция или съвкупност от операции, извършвана с лични данни или набор от лични данни чрез автоматични или други средства като събиране, записване, организиране, структуриране, съхранение, адаптиране или промяна, извличане, консултиране, употреба, разкриване чрез предаване, разпространяване или друг начин, по който данните стават достъпни, подреждане или комбинирание, ограничаване, изтриване или унищожаване.

4. **„Администратор на лични данни“** означава физическо или юридическо лице, публичен орган, агенция или друга структура, която сама или съвместно с други определя целите и средствата за обработването на лични данни; когато целите и средствата за това обработване се определят от правото на Съюза или правото на държава членка, администраторът или специалните критерии за неговото определяне могат да бъдат установени в правото на Съюза или в правото на държава членка.



5. **„Обработващ лични данни“** означава физическо или юридическо лице, публичен орган, агенция или друга структура, която обработва лични данни от името на администратора.

6. **„Получател“** означава физическо или юридическо лице, публичен орган, агенция или друга структура, пред която се разкриват личните данни, независимо дали е трета страна или не. Публичните органи, които могат да получават лични данни в рамките на конкретно разследване в съответствие с правото на Съюза или правото на държава членка, не се считат за „получатели“; обработването на тези данни от посочените публични органи отговаря на приложимите правила за защита на данните съобразно целите на обработването.

7. **„Съгласие на субекта на данните“** означава всяко свободно изразено, конкретно, информирано и недвусмислено указание за волята на субекта на данните, посредством изявление или ясно потвърждаващо действие, което изразява съгласието му свързаните с него лични данни да бъдат обработени.

8. **„Регистър с лични данни“** означава всеки структуриран набор от лични данни, достъпът до които се осъществява съгласно определени критерии, независимо дали е централизиран, децентрализиран или разпределен съгласно функционален или географски принцип.

9. **„Нарушение на сигурността на лични данни“** означава нарушение на сигурността, което води до случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или достъп до лични данни, които се предават, съхраняват или обработват по друг начин.

10. **„Надзорен орган“** означава независим публичен орган, създаден от държава членка съгласно член 51 от Регламента, който е отговорен за наблюдението на прилагането на Регламента, за да се защитят основните права и свободи на физическите лица във връзка с обработването и да се улесни свободното движение на личните данни в рамките на Съюза. В Република България този надзорен орган е Комисия за защита на личните данни с контакти: София, п.к. 1592, бул. „Проф. Цветан Лазаров” № 2, тел. 02/91-53-518, електронна поща: [kzld@cpdp.bg](mailto:kzld@cpdp.bg)

### Лични данни, обработвани в БААТ

БААТ като администратор обработва лични данни, предоставени от физическите лица, за които се отнасят данните, във връзка със:

- сключване на договори с партньори и доставчици;
- сключване на граждански договори;
- публично достъпни регистри, например Търговския регистър;



- отчитане на дейността на Сдружението
- провеждане на общи събрания и годишни срещи
- провеждане на обучения, семинари и работни събития

Категории лични данни, които се обработват от администратора, са данни за:

- **физическа идентичност:** имена, електронен адрес, ЕГН, телефон;
- **социална идентичност:** длъжност
- банкова сметка;

## Обработване на лични данни.

Като администратор на лични данни БААТ обработва лични данни чрез съвкупност от действия, които могат да се извършват по отношение на личните данни с автоматични или други неавтоматични средства, събиране, записване, организиране, структуриране, съхранение, адаптиране или промяна, извличане, консултиране, употреба, разкриване чрез предаване, разпространяване или друг начин, по който данните стават достъпни, подреждане или комбиниране, ограничаване, изтриване или унищожаване, при спазване на следните принципи:

### 1. Законосъобразност, добросъвестност и прозрачност

Сдружението обработва личните данни законосъобразно, добросъвестно и по прозрачен начин по отношение на субектите на данни.

### 2. Ограничение на целите

Сдружението събира личните данни за конкретни, изрично указани и легитимни цели и не се обработват по-нататък по начин, несъвместим с тези цели.

### 3. Свеждане на данните до минимум

Личните данни трябва да бъдат подходящи, свързани със и ограничени до необходимото във връзка с целите, за които се обработват. По възможност Сдружението прилага криптиране или псевдонимизация на личните данни, за да ограничи рисковете за субектите на данни.

### 4. Точност и актуалност

Личните данни трябва да са точни и при необходимост да бъдат поддържани в актуален вид. Сдружението предприема всички разумни мерки, за да гарантира своевременното изтриване или коригиране на неточни лични данни, като се имат предвид целите, за които те се обработват.

### 5. Ограничение на съхранението



Сдружението съхранява личните данни във форма, която да позволява идентифицирането на субекта на данните за период, не по-дълъг от необходимото за целите, за които се обработват личните данни.

## **6. Цялостност и поверителност**

Сдружението обработва личните данни по начин, който гарантира подходящо ниво на сигурност на личните данни, включително защита срещу неразрешено или незаконосъобразно обработване и срещу случайна загуба, унищожаване или повреждане, като се прилагат подходящи технически или организационни мерки.

## **7. Отчетност**

Сдружението носи отговорност и е в състояние да докаже спазването на всички принципи на Регламента, приети и с настоящата Политика.

Сдружението гарантира, че отговаря на всички тези принципи както при обработването на лични данни, което извършва в момента, така и като част от въвеждането на нови средства за обработване, като например нови информационни системи.

БААТ обработва личните данни самостоятелно или чрез възлагане на обработващи данните, като определя целите и обемът на задълженията, възложени от администратора на обработващия данните, при наличие на релевантно правно основание, съгласно изискванията на Регламента и съобразявайки се с националното законодателство.

### **Цел на обработката на лични данни.**

Целта на обработка на лични данни е еднозначно да се идентифицират физическите лица.

Обработката на данни е в следствие на изпълнение на нормативно установени задължения на администратора на лични данни, произтичащи от изискванията на законодателството, финансово-счетоводната дейност, установяване на трайни търговски взаимоотношения, Устава на сдружението.

Обработването на лични данни от Сдружението е допустимо освен в горните случаи, така и когато физическото лице, за което се отнасят данните, е дало изрично своето съгласие или обработването е необходимо за изпълнение на задължения по договор, по който физическото лице, за което се отнасят данните, е страна, както и за действия, предхождащи сключването на договор и предприети по искане на лицето, както и за целите на легитимните интереси на администратора или на трета страна.

### **Използването на личните данни за друга цел (освен първоначалната)**



Сдружението декларира, че личните данни се обработват само за целите, за които първоначално са били събрани. В случай, че възникне необходимост събраните данни да се обработват за друга цел, Сдружението ще направи индивидуална преценка за съвместимостта на целите за всеки един конкретен случай, както и ако е необходимо, ще потърси съгласието на своите субекти на данни в ясна и кратка форма.

Сдружението включва във всяко такова искане първоначалната цел, за която са събрани данните, както и новата или допълнителната/ите цел/и. Искането включва и причината за промяната на целта/целите.

### Обработване на лични данни на основание „съгласие“ на субекта на данни

Сдружението спазва всички изисквания на Регламента за личните данни, събирани и обработвани на правно основание съгласие на субекта на данни.

Когато обработването на лични данни се основава на съгласието на субекта на данните, натовареното длъжностно лице е отговорно за запазването на това съгласие. Също така носи отговорност за предоставянето на съгласието на субектите на данни, които трябва да дадат съгласието си и трябва да информира и да гарантира, че тяхното съгласие може да бъде оттеглено по всяко време.

### Разкриване на лични данни

Сдружението, като администратор на лични данни има право да разкрие обработваните лични данни само на следните изчерпателно изброени категории лица:

1. физически лица, за които се отнасят данните;
2. лица, за които правото на достъп е предвидено в нормативен акт или
3. лица, за които правото произтича по силата на договор.

### Права на субектите на данни

Физическите лица, чиито лични данни се обработват имат следните права:

1. **Право на информираност**, относно данните, които идентифицират администратора и координатите за връзка с него, и когато е приложимо, тези на представителя на администратора, целите на обработването на личните данни, както и правното основание за обработването, законните интереси на администратора, в случай, че обработването се извършва на това основание, получателите или категориите получатели, на които могат да бъдат разкрити данните, задължителния или доброволния характер на предоставяне на данните и последиците от отказ за предоставянето им, срока, за който ще се съхраняват личните данни, съществуването на право да се изиска от администратора достъп до, коригиране или изтриване на лични данни или ограничаване на обработването на лични данни, свързани със субекта на данните, или право да се направи възражение срещу обработването, както и правото на преносимост на данните, правото на жалба до надзорен орган.



2. **Право на достъп** до отнасящи се до физическото лице данни.
3. **Право на коригиране** на неточни лични данни, свързани с физическото лице.
4. **Право на изтриване (право “да бъдеш забравен”)** на свързаните с физическото лице лични данни при спазване на изискванията на чл.17 от Регламента.
5. **Право на ограничаване на обработването** на данните, свързани с физическото лице при спазване на изискванията на чл.18 от Регламента.
6. **Право на преносимост на данните** в структуриран, широко използван и пригоден за машинно четене формат, както и прехвърляне на тези данни на друг администратор без възпрепятстване от администратора, на когото личните данни са предоставени.
7. **Право на възражение.** Субектът на данните има право, по всяко време и на основания, свързани с неговата конкретна ситуация, на възражение срещу обработване на лични данни, отнасящи се до него, което се основава на задача от обществен интерес, упражняване на официално правомощие или на легитимен интерес, включително профилиране, основаващо се на посочените основания. Администраторът прекратява обработването на личните данни, освен ако не докаже, че съществуват убедителни законови основания за обработването, които имат предимство пред интересите, правата и свободите на субекта на данни, или за установяването, упражняването или защитата на правни претенции.
8. **Право на жалба** до надзорния орган.

Сдружението съдейства на субектите на данни при упражняването на техните права, като ги информира за тях и се стреми да удовлетвори исканията им и да им даде отговор в законоустановения срок, когато тези искания са основателни.

#### Ред за упражняване на права.

Физическите лица, упражняват правата си, като подават писмено заявление (включително чрез електронни средства), както и устно (по телефона или на място в канцеларията на Сдружението) до Сдружението, съдържащо минимум следната информация:

11. име, адрес и други данни за идентифициране на съответното физическо лице;
12. описание на искането;
13. до кои лични данни се отнася искането;
14. предпочитана форма за предоставяне на информацията;
15. подпис, дата на подаване на заявлението и адрес за кореспонденция.

Искането може да бъде подадено и по електронен път, като бъде подписано по реда на Закона за електронния документ и електронния подпис.



Подаването на заявление е безплатно.

При подаване на заявление от упълномощено лице, към заявлението се прилага и изрично нотариално заверено пълномощно.

В случай на смърт на физическото лице, правата му се упражняват от неговите наследници, като към заявлението се прилага удостоверение за наследници.

Когато са подадени искания за упражняване на права от субекти на данни, отговорното длъжностно лице в Сдружението трябва да гарантира, че тези искания се обработват в разумен срок.

Отговорното длъжностно лице също трябва да записва исканията и да води дневник за тях.

### Трансфер на лични данни

Сдружението се задължава предаването на лични данни, които се обработват или са предназначени за обработване след предаването на трета държава или на международна организация, да се осъществява само при условие, че са спазени разпоредбите на Регламента, включително във връзка с последващи предавания на лични данни от третата държава или от международната организация на друга трета държава или на друга международна организация, за да се осигури необходимото ниво на защита на физическите лица по Регламента и те да не бъдат изложени на риск.

### Ключови длъжности и отговорности във връзка със защитата на личните данни

Управителният орган на Сдружението формулира задълженията на лицата и нивото на достъп до личните данни, които се обработват.

### Мерки за защита на личните данни

Сдружението приема принципа за защита на личните данни на етапа на проектирането и гарантира, че определянето, планирането и изграждането на всички нови или значителната промяна на вече съществуващи системи, които събират или обработват лични данни, ще бъдат обект на надлежна преценка, свързана със защитата на личните данни.

Сдружението организира и осигурява някои или всички от следните видове защита на личните данни от случайно или незаконно унищожаване, от неправомерен достъп, от изменение или разпространение, както и от други незаконни форми на обработване.



- **Физическа** – осигуряване на технически и организационни мерки по защита на сградите, помещенията и съоръженията, в които се събират, обработват и съхраняват лични данни, и контролиране на достъпа до тях.
- **Персонална** – осигуряване на организационни мерки спрямо физическите лица, които обработват лични данни по указание на администратора, гарантираща достъпа до лични данни само на лица, чиито служебни задължения или конкретно възложена задача налагат такъв достъп.
- **Документална** – осигуряване на система от организационни мерки при обработването на лични данни на хартиен носител.
- **Защита на автоматизираните информационни системи и/или мрежи** – осигуряване на система от технически и организационни мерки за защита от незаконни форми на обработване на личните данни. Поддържане на компютърни работни конфигурации на съвременно техническо ниво. Сдружението се ангажира да използва технически мерки като псевдонимизация, криптиране, свеждане на данните до минимум и други подходящи мерки за защита на личните данни, когато е осъществимо и приложимо.

## Уведомления и съобщения при нарушение на сигурността на личните данни

Политиката на Сдружението е да се спазват принципите на добросъвестност и пропорционалност, когато се обсъжда какви действия да бъдат предприети, за да се информират засегнатите страни при нарушение на сигурността на личните данни. В съответствие с Регламента, когато е налице нарушение, което може да доведе до риск за правата и свободите на физическите лица, Сдружението ще информира надзорния орган в рамките на 72 часа от узнаване на нарушението от страна на Сдружението.

## Отговорност.

Всички лица, заети по трудов или граждански договор при администратора, както и изрично оправомощените от него лица, обработващи лични данни, са длъжни да спазват настоящата Политика за защита на личните данни и предвиденото в същата, като за изпълнение на това задължение носят отговорност по Закона за защита на личните данни и Кодекса на труда, както и всички други законови и подзаконови нормативни актове в Република България, касаещи защитата на личните данни на физическите лица.

## Заклучителни положения

Следните действия са предприети, за да се гарантира, че по всяко време Сдружението спазва принципа на отчетност по Регламента:



- Правната основа за обработването на личните данни е ясна и недвусмислена.
- Всички служители, които под една или друга форма боравят с лични данни, разбират своята отговорност за спазване на добрите правила и практики за защита на личните данни.
- Всички служители са преминали обучение по защита на личните данни.
- Спазват се правилата, свързани със съгласието.
- Въведена е процедура, по която субектите на данни могат да упражнят своите права по отношение на личните си данни и техните искания се обработват своевременно и ефективно.
- Извършва се редовен периодичен преглед на процедурите, свързани с лични данни.
- Спазват се всички предприети мерки за защита на личните данни;
- Следната информация се поддържа в актуален вид:
  - Име на организацията и координати за връзка;
  - Цели на обработването на лични данни;
  - Категории лица и лични данни, които се обработват;
  - Категории получатели, на които личните данни се разкриват;
  - Срокове за съхранение на личните данни;
  - Прилагани технически и организационни мерки за защита на данните
- В случай на възникнала необходимост и наличие на трансфер на данни, по смисъла на Регламента, Сдружението ще предприеме необходимите действия за съответствие със Регламента и поддържане в актуален вид на споразумения и механизми за трансфер на лични данни към държави извън ЕС, включително подробности за въведените мерки за контрол.

Настоящата политика е приета от Управителния съвет на Сдружението на 12 април 2018 г.

Подлежи на преглед и актуализация най-малко веднъж годишно, както и при промени в приложимото законодателство.