Политика за защита на личните данни при предоставяне на Удостоверителни услуги

Идентификатор: **PL-PD-1**
Версия: **1 / 01.05.2025**
Гриф: **C1 / ОБЩОДОСТЪПЕН ДОКУМЕНТ**

Съдържание:

1. Въведение 3

2. Термини и съкращения 3

3. Администратор на личните данни 4

4. Обработвани лични данни в зависимост от начина на предоставяне на удостоверителни услуги 4

4.1 За услуги, предоставяни при лично явяване в офис на Регистриращ орган на БОРИКА АД 5

4.2 За услуги, предоставяни чрез мобилното приложение B-Trust Mobile 5

4.3 При идентификация от разстояние чрез уеб интерфейс.....6

5. Цели на обработката 7

6. Основания за обработка..... 7

7. Съхранение на личните данни 8

8. Права на субектите на данни 10

9. Мерки за сигурност на личните данни 11

10. Разкриване на лични данни..... 12

11. Международно предаване на лични данни 13

12. Контакти..... 13

1. Въведение

Настоящата политика има за цел да опише начина, по който се събират, обработват и съхраняват личните данни и е приложима към предоставяните от „БОРИКА“ АД удостоверителни услуги.

Всички изменения и допълнения в настоящата политика ще бъдат прилагани след публикуването им на уебсайта: **http://www.b-trust.bg**.

2. Термини и съкращения

Администратор на лични данни – всяко физическо или юридическо лице, което определя целите и средствата за обработването на лични данни. Ако целите и средствата за това обработване се определят от законодателството на Европейския съюз или на държава членка, тогава администраторът или критериите за определянето му могат да бъдат посочени в това законодателство.

Лични данни са всякаква информация, която се отнася до физическо лице, което е идентифицирано или може да бъде идентифицирано („субект на данни“). Идентификацията може да бъде пряка или непряка – например чрез име, идентификационен номер, данни за местоположение, онлайн идентификатор или чрез един или повече признаци, характерни за физическата, физиологичната, генетичната, психическата, умствената, икономическата, културната или социалната идентичност на лицето.

Обработване на лични данни - всяко действие или съвкупност от действия, извършвани с лични данни или с набор от лични данни – независимо дали чрез автоматични или други средства, които включват дейности като събиране, записване, използване, разкриване чрез предаване, а също и разпространение или предоставяне на достъп до данните по друг начин, както и подреждане, комбиниране, ограничаване, изтриване или унищожаване.

Псевдонимизация – обработване на лични данни по начин, който не позволява свързването им с конкретно физическо лице без използването на допълнителна информация. Тази допълнителна информация трябва да се съхранява отделно и да бъде обект на подходящи технически и организационни мерки, които гарантират, че личните данни не могат да бъдат свързани с идентифицирано или подлежащо на идентификация лице.

Субекти на данни - физически лица, които в лично качество или като законни/ упълномощени представители на физическо или юридическо лице заявяват и/или ползват удостоверителните услуги на БОРИКА АД и чиито данни се обработват във връзка с предоставянето на удостоверителни услуги и сключването на договор (наричани за краткост „клиенти“).

Съгласие на субекта на данните - всяко свободно изразено, конкретно, информирано и недвусмислено изразяване на волята на субекта на данните,

направено чрез изявление или ясно потвърждаващо действие, с което се дава съгласие за обработване на свързаните с него лични данни.

Приложима нормативна уредба - включва нормативни актове на Европейския съюз, в това число, но не само: Общия регламент за защита на данните (ЕС) 2016/679 (GDPR), Закона за защита на личните данни, Закона за електронния документ и електронните удостоверителни услуги, както и всеки друг нормативен акт, приложим към обработването на лични данни.

Регистриращ орган - обособена структура на БОРИКА АД или външно юридическо лице (подизпълнител), на което дружеството възлага извършването на услуги по регистрация, идентификация и удостоверяване на самоличност/идентичност на потребители.

3. Администратор на личните данни

БОРИКА АД е администратор на личните данни по смисъла на приложимото законодателство. Дружеството е със следните данни за идентификация:

- ЕИК 201230426
- Седалище и адрес на управление: гр. София 1612, р-н Красно село, бул. „Цар Борис“ III № 41
- Уебсайт: http://www.borica.bg
- Имейл: office@borica.bg
- Контактен център: support@borica.bg
- Телефон: 0700 199 10, *9910

4. Обработвани лични данни в зависимост от начина на предоставяне на удостоверителни услуги

В зависимост от начина, по който се заявяват и предоставят удостоверителните услуги, БОРИКА АД обработва различни лични данни, включително идентификационни, контактни, биометрични и платежни данни, както е описано по-долу:

4.1 За услуги, предоставяни при лично явяване в офис на Регистриращ орган на БОРИКА АД

За идентификация и потвърждаване на самоличността при предоставяне на удостоверителни услуги се обработват:

- Имена (по документ за самоличност), ЕГН/личен номер на чужденец, дата на раждане (за чужденци), адрес, телефон, електронна поща;
- Данни за пълномощник (имена, ЕГН, адрес и други, съдържащи се в документа за упълномощаване);
- Номер, дата на издаване и срок на валидност на документа за самоличност;
- Данни, извлечени от национални регистри на първични администратори на данни при извършване на служебна проверка на валидността на документа за самоличност и жизнения статус, както иавтоматично извлечени данни от машинно четимата част на документа;
- Данни от извършени плащания на клиента за предоставени услуги – номер на банкова сметка и друга платежна информация.

4.2 За услуги, предоставяни чрез мобилното приложение B-Trust Mobile

Обработват се следните данни за идентификация и потвърждаване на самоличността:

- Имена (по документ за самоличност), ЕГН, номер, дата на издаване и валидност и издател на документ за самоличност, пол, дата на раждане, националност, адрес, телефон, електронна поща;
- Биометрични данни:
  - електронно копие (снимки) на документа за самоличност, включително всички автоматично свалени данни от машинно четимата му част;
  - видео запис на лицето с произнесен от него текст/код;
  - снимка на лицето, извлечена от националните регистри на първични администратори на данни;
- Данни от националните регистри на първични администратори на данни при извършване на автоматизирана служебна проверка на валидността на документа за самоличност и жизнения статус;
- Данни от националните регистри на първични администратори на данни при инициирана от клиента или доверяваща се страна услуга за електронна идентификация;
- Доклад от проверка и потвърждаване на самоличност на физическо лице при отдалечена видео идентификация с резултати за наличие или липса на съответствие между сканирания документ за самоличност, данните от извършената служебна проверка и видео записа;

- Данни, използвани при подписване на електронни документи чрез B-Trust Mobile, (ЕГН, телефон, електронна поща);
- Данни, събрани при автентикация в системи и приложения;
- Данни от извършени плащания на клиента за предоставени услуги – номер на банкова сметка и друга платежна информация.

Ако клиентът използва приложението B-Trust Mobile, то той преминава през процес на регистрация и отдалечена видео идентификация. Преди началото на процеса по отдалечена идентификация е необходимо клиентът доброволно да предостави личните си данни (вкл. биометрични), които ще бъдат обработени, за да се ползват удостоверителни услуги чрез приложението. Клиентът потвърждава, че е приел условията за използване на личните му данни с поставяне на отметка (чек-бокс). Това действие, заедно с продължаването на процеса по регистрация, се счита за електронно изявление по смисъла на Закона за електронния документ и електронните удостоверителни услуги и еднозначно указва приемането и задължението за спазване на изискванията в настоящата Политика.

В случай че клиентът желае да ползва услугите B-Trust, но не желае неговите биометрични данни да бъдат обработвани, той може да се идентифицира лично в офис на Регистриращ орган на БОРИКА АД и да заяви удостоверителни услуги, които не изискват използване на мобилно приложение.

4.3 При идентификация от разстояние чрез уеб интерфейс

За предоставяне на определени услуги, включително сключване на договори чрез електронен канал, Дружеството събира, обработва и съхранява следните лични данни на клиента:

1. Идентификационни данни:

- Имена по документ за самоличност;
- ЕГН (или друг национален идентификационен номер съгласно държавата на издаване);
- Номер, дата на издаване, валидност и издател на документа за самоличност;
- Националност, пол, дата на раждане;
- Адрес, телефонен номер и електронна поща.

2. Биометрични данни:

- Електронно копие (снимки) на документа за самоличност, включително данни, извлечени от машинно четимата му част;
- Видео запис и снимки, направени по време на процеса на идентификация, включително запис на произнесен текст/код;
- Снимки, извлечени от официални национални регистри, при наличие на свързаност.

3. Данни от официални регистри:

- Данни, извлечени при автоматизирана проверка на валидността на документа за самоличност и жизнения статус;
- Данни, свързани с проверка на съответствие между предоставените данни и данните от национални регистри, включително снимкови съвпадения.

4. Доклад за идентификация:

- Резултат от проверката и потвърждаване на самоличност, включително степен на съответствие между предоставените и официално получените данни.

Клиентът потвърждава, че е приел условията за използване на личните му данни с поставяне на отметка (чек-бокс). Това действие, заедно с продължаването на процеса по регистрация се счита за електронно изявление по смисъла на Закона за електронния документ и електронните удостоверителни услуги и еднозначно указва приемането и задължението за спазване на изискванията в настоящата Политика.

5. Цели на обработката

БОРИКА АД обработва лични данни на клиентите си със следните цели:

- Предоставяне на удостоверителни услуги и управление на взаимоотношенията с клиентите;
- Получаване на информация, необходима за сключване на договор за услуги;
- Идентифициране и потвърждаване на самоличността на клиент при ползване на удостоверителни услуги B-Trust;
- Отговори на искания за предоставяне на информация, за отговори по жалби, оспорвания и разяснения за ползваните услуги, справки за ползвани услуги;
- Предпазване на клиентите, ползващи удостоверителни услуги B-Trust, от измами и злоупотреби от трети лица;
- Актуализиране на лични данни, предоставени при регистрация/сключване на договор за услугите и продуктите B-Trust;
- Техническо съдействие и поддръжка при ползване на удостоверителни услуги B-Trust, предоставено по телефон, електронна поща или на място;
- Изпълнение на законови задължения, решаване на спорове пред компетентния орган (съд, арбитраж, помирителна комисия, административни органи и др.), във връзка с дейността на БОРИКА АД.

6. Основания за обработка

БОРИКА АД обработва лични данни на клиентите си на следните основания:

- **Законово задължение**

За изпълнение на законови задължения по идентифициране на клиенти, както и за извършване проверки по идентификацията, в съответствие с Регламент (ЕС) № 910/2014 относно електронната идентификация и удостоверителните услуги, Закона за мерките срещу изпиране на пари и Закона за платежните услуги и платежните системи.

- **Изпълнение на договорни отношения**

  За надлежна идентификация при сключване на договор и по време на действието му. Обработването се извършва, за да се осигури правомерно ползване на договорения продукт или услуга, включително известяване за всички важни промени при ползването им.

- **Легитимен интерес**
  - за подобряване на продуктите и услугите в съответствие с потребностите и изискванията на клиентите, както и за подобряване на клиентското обслужване;
  - за предотвратяване на измами или изпиране на пари, с цел защита на бизнеса и съобразяване с приложимите закони;
  - при видеонаблюдение за събиране на доказателства при възникване на криминални ситуации, както и за защита на клиентите и служителите;
  - при електронна кореспонденция и телефонни записи (например при сигнали, уведомления за изгубени сертификати за електронни подписи или при запитвания към контактен център);
  - при изпращане на съобщения за ползваните продукти и услуги чрез SMS известия, които не са свързани с маркетингови цели;
  - при жалби и за удовлетворяване на искания, при спорове, свързани с ползването на удостоверителни или платежни услуги.

- **Съгласие на Клиента**

  В случаите когато БОРИКА АД обработва данни на основание изрично съгласие от страна на клиента, обработването се извършва само за посочените в съгласието цели и данни. Всяко дадено съгласие може да бъде оттеглено по всяко време, без това да засяга законосъобразността на обработването преди оттеглянето.

7. Съхранение на личните данни

Срокът за съхранение на личните данни зависи от целите на обработването, за които са събрани. БОРИКА АД обработва лични данни за сроковете, установени в действащото в страната законодателство. Лични данни, за които липсва изрично законово задължение за съхранение, се изтриват след постигане на целите, за които са събрани и обработени. Някои срокове могат да бъдат удължени при възникване на определени обстоятелства: например, при случаи на съдебни дела, при

удължаване на давностен срок поради прекъсване, при изпълнение на специфични законови разпоредби и/или изисквания на надзорни органи.

Данните, подадени при заявка за издаване на електронен подпис, която не е реализирана, се съхраняват до 3 месеца след подаването на заявката с оглед завишаване на вниманието на служителите на дружеството за евентуални опити за измама, след което се изтриват.

Данните, използвани по силата на Закона за електронния документ и електронни удостоверителни услуги, се съхраняват 10 години.

Типове данни	**Срок на съхранение**
Лични данни, събирани и съхранявани за предоставяне на удостоверителни услуги и електронна идентификация	10 години след прекратяване на услугата
Лични данни, събирани във връзка със сключването и изпълнението на договори	10 години след прекратяване на договора
Лични данни събирани през процес по успешна отдалечена идентификация	10 години след прекратяване на услугата
Лични данни, събирани, обработвани през процес по неуспешна отдалечена идентификация	3 месеца от извършването ѝ
Лични данни, събирани и съхранявани във връзка с използването на услугата за квалифицирано съхранение на електронно подписани документи (с хранилище)	Тези данни се съхраняват до изтриването им от клиента или до прекратяването на съответната услуга, но не за повече от 10 години
Информация, съдържаща се в комуникация с клиенти във връзка с услугите	10 години след прекратяване на услугата
Запис на телефонни разговори	до 5 години от датата на провеждане на съответния разговор
Финансови и счетоводни документи	До 10 години след началото на годината след плащането
Системни логове	До 3 години от генерирането на лог
Данни, обработвани въз основа на съгласие	До оттегляне на съгласието

8. Права на субектите на данни

Субектите на данни (клиентите) имат следните права:

- **Право на достъп до личните данни**

  Клиентът може да поиска достъп до всичките си лични данни, които се съхраняват в БОРИКА АД. Това е така наречената "заявка за личен достъп". Достъпът до личните данни може да се получи по съответен ред при поискване, както е посочено по-долу.

- **Право на коригиране на неточни или непълни данни**

  Клиентът има правото да изисква от БОРИКА АД да коригира неговите лични данни.

- **Право на изтриване ("право да бъдеш забравен")**

  Клиентът има право да изисква от БОРИКА АД да изтрие без ненужно забавяне неговите лични данни и това ще се извърши, ако са приложими условията на чл. 17 от Общия регламент за защита на данните ЕС 2016/679 (GDPR).

- **Право на ограничаване на обработката**

  Клиентът има право да изисква от БОРИКА АД да ограничи обработването на неговите лични данни или да направи възражение срещу обработването на тези данни.

- **Право на преносимост на данните**

  Клиентът има правото на преносимост за неговите лични данни, ако това е приложимо, съгласно Чл. 20 от Общия регламент за защита на данните ЕС 2016/679 (GDPR).

- **Право на жалба до надзорен орган**

  Клиентът има право да подаде жалба до надзорния орган – Комисията за защита на личните данни, по отношение на неговите лични данни, които е предоставил на БОРИКА АД.

  Клиентът може да упражни своите права като предяви своите искания към БОРИКА АД в писмен вид – на хартиен носител или чрез електронна поща, като използва следните канали за контакт:

  Пощенски адрес: София 1612, бул. „Цар Борис III" 41

  Електронна поща: office@borica.bg

При подаване на писмено искане, клиентът следва недвусмислено да удостовери самоличността си и притежанието на идентификатора, с който е регистриран за ползване на услугите.

Ако клиентът не е съгласен с начина, по който се управляват или използват личните му данни, желае да получи допълнителна информация или да сигнализира за евентуални нарушения на правата си, може да подаде запитване (искане, оплакване,

сигнал) през посочените по-горе канали за контакт. Всички постъпили запитвания се обработват в рамките на един календарен месец.
В случай че БОРИКА АД не предостави удовлетворяващ отговор или решение, клиентът има право да се обърне към Комисията за защита на личните данни на следния адрес:
София 1592, бул. „Проф. Цветан Лазаров" № 2
Електронна поща: kzld@cpdp.bg,
Уебсайт: www.cpdp.bg

9. Мерки за сигурност на личните данни

БОРИКА АД прилага цялостен подход за защита на личните данни, включващ следните мерки за сигурност:

- **Технически мерки:**
  - *Шифроване*: Използване на криптографски технологии за защита на чувствителна информация при съхранение и предаване;
  - *Антивирусен софтуер:* Приложим на сървъри и работни станции. Използва се корпоративна версия на софтуера, редовно актуализирана;
  - *Мрежова защита (Firewalls):* Прилагат се на ключови места в корпоративната мрежа за контрол на входящия и изходящия трафик и предотвратяване на неоторизиран достъп;
  - *Контрол на логическия достъп:* Използване на силни пароли, многофакторна автентикация, адекватни политики за сигурност. Ограничаване на достъпа до лични данни само до оторизирани служители.
  - *Редовни актуализации на софтуера:* Поддържане на операционните системи и приложенията в актуално състояние с цел предотвратяване на уязвимости;
  - *Непрекъсваемост на дейността:* Поддържане на резервни копия на данни с цел бързо възстановяване на работните процеси и услугите, с минимални загуби на данни.
- **Организационни мерки:**
  - *Политики за сигурност*: Документирани вътрешни правила за сигурност и Политика за защита на личните данни, приложими към процесите за обработка и съхранение на лична информация;
  - *Обучение на служителите:* Провеждане на регулярни обучения относно добри практики в областта на киберсигурността и защитата на лични данни;
  - *Оценка на риска:* Оценка и анализ на потенциални рискове, заплахи и уязвимости и прилагане на подходящи мерки за ограничаване на рисковете;
  - *Споразумения за конфиденциалност:* Изискване за подписване на споразумения за поверителност от служители и трети страни;

- *План за реагиране при инциденти:* Прилаган и редовно тестван план за действие при инциденти, свързани със сигурността, в това число при изтичане на данни, включително процедури за уведомяване на засегнатите лица и регулаторните органи;

- **Физически мерки**
  - *Ограничен физически достъп:* Критичните системи се намират в зони с висока степен на сигурност, със система за контрол на достъпа и видеонаблюдение;
  - *Сигурно унищожаване на данни*: Използване на специализирани методи за унищожаване на документи и електронни носители с лична информация;
  - *Мониторинг*: Прилагане на средства за непрекъснато наблюдение на всички работни пространства, осигуряване на контрол върху използването на преносими средства за съхранение на информация.

БОРИКА АД разглежда защитата на личните данни като основен приоритет, като притежава следните международно признати сертификати:

- ISO/IEC 27001 – Сигурност на информацията, киберсигурност и защита на поверителността;
- ISO/IEC 20000-1 – Информационни технологии. Управление на услуги;
- ISO 22301 – Сигурност и устойчивост. Системи за управление на непрекъснатостта на дейността;
- ISO 9001 – Системи за управление на качеството;
- eIDAS – Регламент относно електронната идентификация и удостоверителните услуги.

10. Разкриване на лични данни

В съответствие с изискванията на Регламент (ЕС) 2016/679, БОРИКА АД може да разкрива лични данни, които обработва, на следните категории получатели:

- На самите субекти на данни (физически лица);
- На трети страни - физически и юридически лица, публични органи, институции и учреждения, външни и вътрешни одитори, застрахователни дружества, надзорни и регулаторни органи, при изпълнение на законови или договорни задължения на БОРИКА АД, в това число за разкриване и предотвратяване на измами и пране на пари;
- На държавни институции, когато това е законосъобразно и изрично се изисква;
- На подизпълнители на БОРИКА АД, включително Регистриращи органи, които предоставят достатъчни гаранции за прилагането на подходящи технически и организационни мерки за спазването на Регламент 2016/679;

- На други страни със съгласието на субекта на данните.

11. Международно предаване на лични данни

В случай че възникне необходимост от предаване на обработвани от БОРИКА АД лични данни на държави извън Европейското икономическо пространство (ЕИП) или на международни организации, се прилагат разпоредбите на Регламент ЕС 2016/679, които задължително се документират с договорни клаузи.

БОРИКА АД не предава лични данни на държави извън Европейския съюз (ЕС) или Европейското икономическо пространство (ЕИП) чрез разкриване или предоставяне на достъп.

12. Контакти

За указания и съдействие при упражняване на правата си, субектите на данни могат да се свържат с БОРИКА АД на имейл: dpo@borica.bg.

Настоящата Политика подлежи на периодичен преглед и актуализация, с цел поддържане на съответствие с нормативните изисквания и добрите практики.