

Утвърдил:
Стефан Стефанов-
изп. директор на
„БАКС 99“ АД
(Заповед № 182/01.10.2018г.)

ВЪТРЕШНИ ПРАВИЛА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ В „БАКС 99“ АД

ОБЩИ ПОЛОЖЕНИЯ

1. „БАКС 99“ АД (наричано по-нататък „Администратор“), като Администратор на лични данни, събира и обработва определена информация за физически лица.
2. Тази информация може да се отнася до служители, кандидати за работа, клиенти, доставчици, контрагенти, бизнес контакти и други физически лица, с които Администраторът има връзка или, иска да установи бизнес контакт.
3. Настоящите Вътрешни правила уреждат как да бъдат събирани, обработвани и съхранявани личните данни, за да отговорят на стандартите в организацията на Администратора и да са в съответствие с правните изисквания.

ПРАВНО ОСНОВАНИЕ

4. Настоящите Вътрешни правила се издават на основание Закона за защита на личните данни и подзаконовите му актове, така както се променят („Българското законодателство“), и Общия регламент относно защитата на данните (ЕС) 2016/679 („GDPR“).
5. Българското законодателство и GDPR предвиждат правила как организациите, вкл. „БАКС 99“ АД, трябва да събират, обработват и съхраняват лични данни. Тези правила се прилагат от Администратора независимо дали се касае за данни, които се обработват електронно, на хартия или на други носител.
6. За да бъде обработването на лични данни в съответствие с правните изисквания, личните данни се събират и използват основателно, съхраняват се сигурно и Администраторът предприема необходимите мерки, за да не бъдат обработваните лични данни обект на неправомерно разкриване.
7. Администраторът на лични данни е запознат с и следва принципите, предвидени в GDPR:
- личните данни се обработват законосъобразно, добросъвестно и прозрачно;

- личните данни се събират за конкретни, изрично указани и легитимни цели и не се обработват по-нататък по начин, несъвместим с тези цели;
- личните данни са подходящи, свързани с и ограничени до необходимото във връзка с целите, за които се обработват;
- личните данни са точни и при необходимост се поддържат в актуален вид;
- личните данни се съхраняват във форма, която да позволява идентифицирането на засегнатите лица за период, не по-дълъг от необходимото за целите, за които се обработват личните данни;
- личните данни са обработвани 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.

ЦЕЛИ НА ВЪТРЕШНИТЕ ПРАВИЛА

8. Настоящите Вътрешни правила целят Администраторът да:

- бъде в съответствие с приложимото законодателство по отношение на личните данни и да следва установените добри практики;
- установи механизмите за водене, поддържане и защита на отчетните регистри;
- установи задълженията на длъжностните лица, обработващи лични данни и/или лицата, които имат достъп до лични данни и работят под ръководството на обработващите лични данни, тяхната отговорност при неизпълнение на тези задължения;
- защитава правата на персонала, клиентите и партньорите;
- бъде открит как съхранява и защитава личните данни на физическите лица;
- установи необходимите технически и организационни мерки за защита на личните данни от неправомерно обработване (случайно или незаконно унищожаване, случайна загуба, неправомерен достъп, изменение или разпространение, както и всички други незаконни форми на обработване на лични данни);
- бъде защитен при риск от нарушения.

ОБХВАТ

9. Настоящите Вътрешни правила се прилагат по отношение на обработване на лични данни на персонал (в това число и кандидати за работа), контрагенти, доставчици, клиенти и партньори.

СЪБИРАНЕ НА ЛИЧНИ ДАННИ

10. „Лични данни“ са всяка информация, свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано („Субект на данни“), а именно:

Администраторът събира лични данни по отношение на следните категории лица:

- лица, представляващи дружествата, с които Администраторът има бизнес взаимоотношения;
- лица за контакт в дружествата, с които Администраторът има бизнес взаимоотношения;
- лица, които са заинтересовани от получаването на информационни услуги-информационен бюлетин, справочници и др.;
- лица, които кандидатстват за работа пред Администратора;
- лица, които са наети от Администратора въз основа на трудов или граждански договор;

ЦЕЛИ НА СЪБИРАНЕТО НА ДАННИТЕ

11. Администраторът събира личните данни във връзка с изпълнението на следните цели:

А/ За изпълнение на дейности, свързани със сключване, съществуване, изменение и прекратяване на договорни правоотношения, вкл. за:

- изготвяне на всякакви документи;
- за установяване на връзка с лицето за контакт по телефон, факс или по всякакъв друг законосъобразен начин;
- за извършване на услуги/доставки и/или приемане на стоки/услуги, за комуникация във връзка с предоставяне и/или получаване на услуги/стоки и за предоставяне на свързаното с тях клиентско обслужване;
- за водене на счетоводна отчетност във връзка с изпълненията по договори, по които Администраторът е страна;
- за обработка на плащания във връзка със сключените договори от Администратора;
- за изпращане на важна информация до субектите във връзка с промени в правилата, условията и политиките на Администратора и/или друга административна информация;

Б/ За маркетингови цели-след получаване на изрично съгласие от субектите на лични данни;

В/ За статистически цели.

Събиране на данните

12. Данни на контрагенти (управители, представители и/или лица за контакт на юридическото лице, както и данни на клиенти физически лица).
13. Личните данни за всяко лице се предоставят доброволно от самите лица и се събират от Администратора в изпълнение на нормативно задължение, във връзка със сключването на договор и/или изпълнения на задълженията по сключен договор съгласно разпоредбите на Търговския закон, Закона за счетоводството, Закона за задълженията и договорите, Закона за данъка върху добавената стойност и др. и условията посочени в търговски договор със съответния клиент чрез: хартиен носител-писмени документи (вкл. пълномощни, договори, запорни съобщения, банкова информация и др.), по електронна поща-предоставени във връзка с изпълнението на търговски договор и/или чрез попълване на форма за контакт. Лицата се уведомяват за „Политика за защита на личните данни“ на Администратора предварително или в момента на получаване на данните им.
14. Данни на персонал (служители по трудови договори или лица наети по граждански договори), като в тази връзка служителите на Администратора, изрично и доброволно, в писмен вид са дали своето съгласие Администратора да събира, обработва и съхранявана личните им данни.
15. Личните данни за всяко лице наето по трудов или граждански договор се предоставят доброволно от самите лица и се събират от Администратора в изпълнение на нормативно задължение, във връзка със сключването на договор и/или изпълнения на задълженията по сключен договор, съгласно разпоредбите на Кодекса на труда, Закона за задълженията и договорите, Кодекса за социално осигуряване и др.

Законни (легитимни) интереси, преследвани от Администратора

16. Обработването на данните се извършва на основание законен (легитимен) интерес и във връзка със сключването, съществуването, изменението и прекратяването на търговски, трудови или граждански договори при прилагането на нормативните изисквания на Търговския закон, Кодекса на труда, Кодекса за социално осигуряване, Данъчно-осигурителния процесуален кодекс, Кодекса на застраховане, Закона за данъците върху доходите на физическите лица, Закона за счетоводството, Закона за задълженията и договорите и др.

Прозрачност. Права на лицата, чиито данни се обработват от Администратора и условия за упражняване на правата на лицата

17. Администраторът предоставя информация на лицата в кратка, прозрачна, разбираема и лесно достъпна форма, на ясен и прост език.

18. Администраторът се стреми да гарантира, че лицата са запознати относно обработваните от него лични данни и, че лицата изцяло и напълно разбират и са информирани във връзка с обработването в съответствие с изискванията на GDPR и Българското законодателство.
19. Администраторът предоставя информацията на лицата писмено или по друг начин, включително, когато е целесъобразно, с електронни средства. Ако лицето е поискало това, информацията може да бъде дадена устно, при положение че идентичността на лицето е доказана с други средства.
20. Администраторът **предоставя на лицата безплатно** информация относно действията, предприети във връзка с искане относно правото им на достъп, коригиране, изтриване, ограничаване на обработването, преносимост, възражение и автоматизирано вземане на решения, без ненужно забавяне и във всички случаи в **срок от един месец от получаване на искането**.
21. При необходимост този срок може да бъде удължен с още два месеца, като се взема предвид сложността и броя на исканията. Администраторът **информира лицето** за всяко такова удължаване **в срок от един месец от получаване на искането**, като посочва и причините за забавянето. Когато съответно лице подава искане с електронни средства, по възможност информацията се предоставя с електронни средства, освен ако лицето е поискало друго.
22. Ако Администраторът не предприеме действия по искането, Администраторът **уведомява лицето**, без забавяне и най-късно **в срок от един месец от получаване на искането** за причините да не предприеме действия и за възможността за подаване на жалба до надзорен орган и търсене на защита по съдебен ред.
23. Когато исканията на лицето са явно неоснователни или прекомерни, по-специално поради своята повторяемост, Администраторът може или:
- да наложи разумна такса, като взема предвид административните разходи за предоставяне на информацията или комуникацията или предприемането на исканите действия, или
 - да откаже да предприеме действия по искането.

Право на достъп на лицата

24. Всяко лице има право да получи от Администратора потвърждение дали се обработват лични данни, свързани с него, и ако е така, да получи достъп до данните и следната информация:
- целите на обработването;
 - съответните категории лични данни;
 - получателите или категориите получатели, пред които са или ще бъдат разкрити личните данни (вкл. в трети държави или международни организации);

- когато е възможно, предвидения срок, за който ще се съхраняват данните, а ако това е невъзможно, критериите, използвани за определянето на този срок;
 - съществуването на право да се изиска от Администратора коригиране или изтриване на лични данни или ограничаване на обработването на лични данни, свързани със засегнатите лица, или да се направи възражение срещу такова обработване;
 - правото на жалба до Комисията за защита на личните данни;
 - право на обезщетение за претърпени вреди;
 - когато личните данни не се събират от самите лица, всякаква налична информация за техния източник;
 - съществуването на автоматизирано вземане на решения, вкл. профилирането, и поне в тези случаи съществена информация относно използваната логика, както и значението и предвидените последствия от това обработване за лицата.
25. Когато личните данни се предават на трета държава или на международна организация, лицата имат право да бъдат информирани относно подходящите гаранции във връзка с предаването.
26. Администраторът предоставя на лицето копие от личните данни, които са в процес на обработване. За допълнителни копия, поискани от лицето, Администраторът може да наложи разумна такса, въз основа на административните разходи.
27. Когато лицето подава искане с електронни средства, по възможност информацията се предоставя в широко използвана електронна форма, освен ако лицето не е поискало друго.

Право на коригиране

28. Всяко лице, чиито данни се обработват от Администратора, има право да поиска от Администратора да коригира без ненужно забавяне неточните лични данни, свързани с него. Като се има предвид целите на обработването лицето има право непълните лични данни да бъдат допълнени.

Право на изтриване (право „да бъдеш забравен“)

29. Всяко лице, чиито данни се обработват от Администратора, има правото да поиска от Администратора изтриване на свързаните с него лични данни без ненужно забавяне, а Администраторът има задължението да изтрие без ненужно забавяне личните данни, когато:
- личните данни повече не са необходими за целите, за които са били събрани или обработвани по друг начин;
 - лицето оттегли своето съгласие, върху което се основава обработването на данните, и няма друго правно основание за обработването;
 - лицето възрази срещу обработването и няма законни основания за обработването, които да имат преимущество;
 - личните данни са били обработвани незаконосъобразно;

- личните данни трябва да бъдат изтрети с цел спазването на правно задължение, което се прилага спрямо Администратора;
- личните данни са били събрани във връзка с предлагането на услуги на информационното общество.

30. Когато Администраторът е направил личните данни обществено достояние и е задължен съгласно предходния член да изтрие личните данни, той, като отчита наличната технология и разходите по изпълнението, предприема разумни стъпки, включително технически мерки, за да уведоми администраторите, обработващи личните данни, че засегнатото лице е поискало изтриване от тези администратори на всички връзки, копия или реплики на неговите лични данни.

Право на ограничаване на обработването

31. Всяко лице, чиито данни се обработват от Администратора, има право да изиска от Администратора ограничаване на обработването, когато се прилага едно от следното:

- точността на личните данни се оспорва от лицето, за срок, който позволява на Администратора да провери точността на личните данни;
- обработването е неправомерно, но субектът на данните не желае личните данни да бъдат изтрети, а изисква вместо това ограничаване на използването им;
- администраторът не се нуждае повече от личните данни за целите на обработването, но субектът на данните ги изисква за установяването, упражняването или защитата на правни претенции;
- субектът на данните е възразил срещу обработването в очакване на проверка дали законните основания на Администратора имат преимущество пред интересите на субекта на данните.

32. Когато обработването е ограничено съгласно горния параграф, такива данни се обработват, с изключение на тяхното съхранение, само със съгласието на субекта на данните или за установяването, упражняването или защитата на правни претенции или за защитата на правата на друго физическо лице или поради основания от обществен интерес.

33. Когато субект на данните е изискал ограничаването на обработването, Администраторът го информира преди отмяната на ограничаването на обработването.

Задължение за уведомяване при коригиране или изтриване на лични данни или ограничаване на обработването

34. Администраторът съобщава за всяко извършено коригиране, изтриване или ограничаване на обработване на всеки получател, на когото личните данни са били разкрити, освен ако това е невъзможно или изисква несъразмерно големи усилия. Администраторът информира субекта на данните относно тези получатели, ако субектът поиска това.

Право на преносимост на данните

35. Субектът на данните има право да получи личните данни, които го засягат и които той е предоставил на Администратора, в структуриран, широко използван и пригоден за машинно четене формат и има правото да прехвърля тези данни на друг администратор без възпрепятстване от Администратора, когато:

(а) Обработването е основано на съгласие във връзка с определени цели или на договорно задължение на субекта или предприемане на стъпки преди сключване на договор и

(б) обработването се извършва по автоматизиран начин.

36. Когато упражнява правото си на преносимост субектът на данните има право да получи пряко прехвърляне на личните данни от един администратор към друг, когато това е технически осъществимо.

Право на възражение

37. Субектът на данните има право, по всяко време и на основания, свързани с неговата конкретна ситуация, на възражение срещу обработването на лични данни, отнасящи се до него (когато обработването е необходимо за изпълнението на задача от обществен интерес или при упражняване на официални правомощия на Администратора, или обработването е за целите на легитимните интереси на Администратора или на трета страна), включително профилиране.

38. 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 имат установяването, упражняването или защитата на правни претенции.

39. Когато се обработват лични данни за целите на директния маркетинг, субектът на данни има право по всяко време да направи възражение срещу обработването на лични данни, отнасящи се до него за този вид маркетинг, което включва и профилиране, доколкото то е свързано с директния маркетинг.

40. Когато субектът на данни възрази срещу обработване за целите на директния маркетинг, обработването на личните данни за тези цели се прекратява.

41. Най-късно в момента на първото осъществяване на контакт със субекта на данните, той изрично се уведомява за съществуването на правото по предходните членове, което му се представя по ясен начин и отделно от всяка друга информация.

ДОСТЪП НА СЛУЖИТЕЛИТЕ НА АДМИНИСТРАТОРА ДО ЛИЧНИ ДАННИ ОТГОВОРНОСТ НА СЛУЖИТЕЛИТЕ

42. Достъп до предоставените лични данни имат само служителите в администрацията на „БАКС 99“ АД, във връзка с изпълнение на служебните им задължения, като са задължени да предприемат съответните мерки за защита на личните данни.
43. За извършено нарушение, във връзка със защитата на личните данни, виновният служител носи дисциплинарна отговорност.

ТЕХНИЧЕСКИ И ОРГАНИЗАЦИОННИ МЕРКИ ЗА ЗАЩИТА НА ДАННИТЕ

44. Защитата на данните на хартиено копие и на електронен носител от неправомерен достъп, повреждане, изгубване или унищожаване се осигурява посредством поредица от вътрешно регулирани технически и организационни мерки, като Администратора има внедрена, система за сигурност на цялата си инфраструктура.
45. Технически мерки за защита на личните данни
- (1) Всички помещения, в които се съхраняват и обработват лични данни, са с контрол на достъпа. Възможните технически средства за контрол на достъпа са:
- охрана на помещенията;
 - устройства за разпознаване чрез магнитна карта и/или ключ;
 - видеонаблюдение с цел охрана в коридори и помещения, в които се съхраняват лични данни;
 - практика на допускане на външни лица до помещенията на Администратора само с придружител от персонала на администратора.
- (2) Помещенията, в които се съхраняват лични данни са надеждно обезопасени посредством противопожарни мерки съгласно българското законодателство.
46. Мерки за документална защита на личните данни
- (1) Администраторът установява процедури по обработване на лични данни, регламентиране на достъпа до данните, процедури по унищожаване и срокове за съхранение, подробно разписани в настоящите Вътрешни правила. За отделни категории данни може да се предвиди псевдонимизиране .
- (2) Размножаването и разпространението на документи или файлове, съдържащи лични данни, се извършва само и единствено от упълномощени служители при възникнала необходимост.
47. Персонални мерки на защита на личните данни
- (1) Преди заемане на съответната длъжност лицата, които имат достъп до лични данни данни:
- поемат задължение за неразпространение на личните данни, до които имат достъп;

- се запознават с нормативната база, Вътрешните правила и Политиката за защита на личните данни на Администратора относно защитата на личните данни;
- преминават обучение за реакция при събития, застрашаващи сигурността на данните;
- са инструктирани за опасностите за личните данни, които се обработват от дружеството;
- се задължават да не споделят критична информация помежду си и с външни лица, освен по установения с настоящите Вътрешни правила ред.

(2) При постъпване на работа всички служители работещи в администрацията на „БАКС 99“ АД преминават обучение за реакция при събития, застрашаващи сигурността на данните, и обучение относно задълженията на дружеството, свързани с обработката на лични данни, и мерките за защита на данните, които следва да предприемат в процеса на работа. Последващи обучения и тренировки на тези служители се провеждат периодично, за да се гарантира познаване на нормативната уредба, потенциалните рискове за сигурността на данните и мерките за намаляването им.

48. Мерки за защита на автоматизирани информационни системи и криптографска защита

(1) Достъп до операционната система, съдържаща файлове с лични данни, имат само лица, чиито служебни задължения или конкретно възложена задача налагат такъв достъп. Достъпът се осъществява чрез парола.

(2) Електронните бази данни са защитени посредством логически средства за защита, като антивирусна програма, която се обновява автоматично, защитни стени (firewalls) и др.

(3) Архивиране на личните данни на технически носител се извършва периодично с оглед съхранение на информацията.

(4) Защитата на електронните данни от неправомерен достъп, повреждане, изгубване или унищожаване, извършени умишлено от лице или в случай на технически неизправности, аварии, произшествия, бедствия, др., се осигурява посредством:

- въвеждане на пароли за компютрите, чрез които се предоставя достъп до личните данни, и файловете, които съдържат лични данни;
- антивирусни програми, проверки за нелегално инсталиран софтуер;
- периодични проверки на целостта на базата данни и актуализиране на системната информация, поддържане на системата за достъп до данните;
- периодично архивиране на данните на технически носители, поддържане на информацията на хартиен носител (архивни копия).

ТРАНСФЕР НА ЛИЧНИ ДАННИ

49. Администраторът не осъществява и няма да осъществява трансфер на лични данни в страни, извън Европейския съюз.

НАРУШЕНИЯ. УВЕДОМЯВАНЕ ЗА НАРУШЕНИЯ

50. Нарушение на сигурността на данни възниква, когато личните данни, за които „БАКС 99“ АД отговаря, са засегнати от инцидент със сигурността, в резултат на който се нарушава поверителността, наличието или целостта на личните данни. В този смисъл нарушение на данните възниква, когато има нарушение на сигурността, водещо до инцидентно или незаконно унищожаване, загуба, изменение, нерегламентирано разкриване на данни, които се предават, съхраняват или обработват по друг начин.
51. В случай на нарушение на сигурността на личните данни незабавно следва да се уведоми :Веселина Стефанова-Мениджър човешки ресурси

Оценка на нарушенията

52. След като съответният служител на „БАКС 99“ АД получи информация за извършено нарушение, то трябва да определи дали конкретното събитие представлява нарушение на лични данни и да уведоми ръководството на Администратора („БАКС 99“ АД) за събитието (в случай, че то не знае).
53. В случай на нарушение на сигурността на личните данни, за което съществува вероятност да породи риск за правата и свободите на физическите лица, Администраторът (чрез съответния служител), без ненужно забавяне и когато е осъществимо - **не по-късно от 72 часа** след като е разбрал за него, **уведомява Комисията за защита на личните данни.**
54. Когато и доколкото не е възможно информацията да се подаде едновременно, информацията може да се подаде поетапно без по-нататъшно ненужно забавяне.
55. Когато има вероятност нарушението на сигурността на личните данни да породи висок риск за правата и свободите на физическите лица, Администраторът без ненужно забавяне, съобщава на засегнатия субект за нарушението.
56. Администраторът документира всяко нарушение на сигурността на личните данни, включително фактите, свързани с нарушението, последиците от него и предприетите действия за справяне с него.

УНИЩОЖАВАНЕ

57. Счетоводната и търговската информация, както и всички други сведения и документи от значение за данъчното облагане и задължителното обществено и здравно осигуряване се съхраняват от Администратора в следните срокове:
- ведомости за заплати- 50 години;
 - счетоводни регистри и финансови отчети- 10 години;
 - документи за данъчно-осигурителен контрол - 5 години след изтичане на давностния срок за погасяване на публичното задължение, с което са свързани;
 - всички останали носители - 5 години.
58. След изтичането на срока за съхранението им носителите на информация (хартиени или технически), които не подлежат на предаване в Националния архивен фонд, могат да се унищожават.
59. След приключване на срока за съхранение данните се унищожават възможно най-бързо посредством унищожаването на хартиените носители чрез шредирание, а на техническия носител - чрез заличаване и изтриване на съответните файлове от компютрите, лаптопите, както и от всякакви други технически и електронни устройства носители на информация, които са в Дружеството („БАКС 99“ АД).
60. Администраторът предприема поредица от вътрешно регулирани технически и организационни мерки, във връзка с унищожаването на данните.

ДОПЪЛНИТЕЛНИ РАЗПОРЕДБИ

По смисъла на настоящите Вътрешни правила:

§ 1. „Администратор на лични данни“ е „БАКС 99“ АД- акционерно дружество, с ЕИК:121817095, като действия от името на администратора осъществява Веселина Стефанова-Мениджър човешки ресурси

§ 2. „Обработка“ 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 по друг начин, по който данните стават достъпни, подреждане или комбиниране, ограничаване, изтриване или унищожаване;

§ 3. Настоящите *Вътрешни правила за защита на личните данни* се актуализират, при изменение на правната уредба, свързана със защитата на личните данни на гражданите на ЕС.

§ 4. Настоящите *Вътрешни правила за защита на личните данни* се утвърждават от Изпълнителния директор на „БАКС 99“ АД и се довеждат до знанието на лицата, които касаят, със Заповед на Изпълнителния директор на Администратора („БАКС 99“ АД).