

ВЪТРЕШНИ ПРАВИЛА ЗА ДЕЙНОСТТА НА „БИЗНЕС КАТАЛОГ” ЕООД ПО ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

Глава първа

ОБЩИ ПОЛОЖЕНИЯ

Чл.1. Настоящите Вътрешни правила уреждат принципите и дейността по гарантиране на неприкосновеността на личността и личния живот чрез осигуряване на защита на физическите лица от неправомерно обработване на свързаните с тях лични данни в процеса на свободното движение на данните в „БИЗНЕС КАТАЛОГ“ ЕООД, наричано по-долу Администратор.

Чл.2. Вътрешните правила регламентират дейностите, които се извършват в „БИЗНЕС КАТАЛОГ“ ЕООД във връзка с обработването на лични данни по смисъла на 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 (Общ регламент относно защитата на данните), Закона за защита на личните данни, както и на подзаконовите нормативни актове в областта.

Глава втора

ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ

Раздел 1

Общи положения

Чл.3.(1) Лични данни са всяка информация, свързана с идентифицирано лице или физическо лице, което може да бъде идентифицирано. Физическо лице, което може да бъде идентифицирано (субект на данни), е лице, което 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 лице.

(2) Личните данни трябва да:

1. се обработват законосъобразно, добросъвестно и по прозрачен начин;
2. се събират за конкретни, изрично указани и легитимни цели и да не се обработват по-нататък по начин, несъвместим с тези цели;
3. бъдат подходящи, свързани със и ограничени до необходимото във връзка с целите, за които се обработват;
4. бъдат точни и при необходимост да се актуализират;
5. се заличават или коригират, когато се установи, че са неточни или непропорционални по отношение на целите, за които се обработват;

6. се съхраняват във вид, който позволява идентифициране на съответните физически лица за период не по-дълъг от необходимия за целите, за които тези данни се обработват;

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

Чл.4.(1) Администраторът на лични данни определя вида на личните данни, целите и средствата за обработването им, освен ако те не са определени със закон.

(2) При осъществяване на дейността по ал. 1, администраторът структурира съвкупност от лични данни за целите на съответните регистри.

Чл. 5. Администраторът предприема необходимите технически и организационни мерки за защита на личните данни, за да гарантира адекватно ниво на защита, което отговаря на обработваните лични данни и въздействието при нарушаване на защитата им.

Раздел 2 **Обработване**

Чл.6. Обработване на лични данни е всяко действие или съвкупност от действия, които могат да се извършват по отношение на личните данни с автоматични или други средства, като събиране, записване, организиране, съхраняване, адаптиране или изменение, възстановяване, консултиране, употреба, разкриване чрез предаване, разпространяване, предоставяне, актуализиране или комбиниране, блокиране, заличаване или унищожаване.

Чл.7.(1) В случаите, когато личните данни се събират от лицето, за което се отнасят, администраторът му предоставя:

1. Данните, които идентифицират администратора и координатите за връзка с него и, когато е приложимо, тези на представителя на администратора.

2. Целите на обработването, за което личните данни са предназначени, както и правното основание за обработването.

3. Получателите или категориите получатели, на които могат да бъдат разкрити данните.

4. Когато основание за обработването е законен интерес на администратора или трета страна, законните интереси, преследвани от администратора или от третата страна.

5. Когато е приложимо, намерението на администратора да предаде личните данни на трета държава или на международна организация.

6. Срока за съхранение на личните данни, а ако това е невъзможно, критериите, използвани за определяне на този срок.

7. Права на субекта на лични данни – право на достъп до, коригиране или изтриване на лични данни или ограничаване на обработването на лични данни, свързани със субекта на данните, право да се направи възражение срещу обработването, както и право на преносимост на данните.

8. Право на оттегляне на дадено съгласие, в случай че съгласието е основание за обработване на лични данни.

9. Право на жалба до надзорен орган.

10. Дали предоставянето на лични данни е задължително или договорно изискване, или изискване, необходимо за сключването на договор, както и дали субектът на данни е длъжен да предостави лични данни и евентуалните последствия, ако тези данни не бъдат предоставени.

(2) Когато администраторът възнамерява по-нататък да обработва лични данни с цел, различна от тази, за която са събрани личните данни, той предоставя на субекта на данните преди това по-нататъшно обработване информация за тази друга цел и всякаква друга необходима информация, както е посочено в ал. 1, т. 6 - 10.

(3) Данните по ал. 1 не се предоставят, когато физическото лице, за което се отнасят, вече разполага с тях.

Чл.8. (1) Администраторът може да възложи обработването на личните данни на негови служители. Обработването може да се възложи на повече от един служител, съобразно спецификата на изпълняваните от тях служебни функции и с цел разграничаване на конкретните им задължения.

(2) Служителят, обработващ лични данни, действа само по указание на администратора, освен ако в закон не е предвидено друго.

Чл.9. (1) Личните данни в регистрите се набират от администратора на лични данни, респективно – от служителите, обработващи лични данни устно и/или на хартиен носител.

(2) Служителите, обработващи данните, информират лицето за необходимостта от набирането на данните и целите, за които ще бъдат използвани, като му предоставят Уведомление за поверително третиране на лични данни. Уведомлението съдържа накратко предвидената в чл. 13 от Общия регламент за защита на личните данни информация.

(3) Уведомлението е поставено на видно място в офиса на Администратора, където се събират личните данни.

(4) На сайта на Администраторът е поместена Политика за защита на личните данни, която е достъпна за всички клиенти на Администратора, която желаят да се запознаят с нея в електронен формат.

Раздел 3 **Регистри на дейността**

Чл. 10. В дружеството са създадени следните регистри на дейността:

1. Регистър „Персонал“.
2. Регистър „Клиенти“.
3. Регистър „Контрагенти“.

Чл. 11. (1) В регистър „Персонал“ се съхраняват лични данни за служителите на дружеството.

(2) Личните данни, които се съхраняват в този регистър са:

- три имена, ЕГН, личен телефон, адрес, данни от документ за самоличност на работника/служителя;
- образование – документ за придобито образование, квалификация, правоспособност;
- трудова дейност – съгласно приложените документи за трудов стаж и професионална биография;
- свидетелство за съдимост, когато се изисква;

(3) Личните данни в регистър “Персонал” се набират при подаване на документи за постъпване на работа по трудово правоотношение, както и при кандидатстване за работа.

(4) Лични данни на кандидати за работа, с които не е сключен трудов договор – 1 месец от заемане на обявената свободна позиция.

(5) Трудовото досие се пази през цялото време на трудовото правоотношение, като след прекратяване на трудовото правоотношение, ведомостите за заплати се пазят за срок от 50 години, считано от 1 януари на отчетния период, следващ отчетния период, за който се отнасят, както е предвидено в Закона за счетоводството.

(6) Лични данни, отнасящи се за използвани при парични обезщетения и помощи се съхраняват за срок от 6 години. Лични данни за използвани в платени отпуски, инструктажи и други документи, извън гореизброените – 6 години след прекратяване на трудовото правоотношение.

(7) Лицата, събиращи и обработващи лични данни в регистър „Персонал“, имат следните права и задължения:

1. да използват личните данни при спазване разпоредбите на Кодекса на труда и Кодекса за социално осигуряване.
2. да използват личните данни за изпълнение на задълженията по Закона за здравното осигуряване /ЗЗО/.
3. да не изнасят и съхраняват личните данни извън специално определените за целта места;
4. да не използват личните данни по нерегламентиран начин /фалшифициране и друг вид злоупотреба/.

Чл. 12. (1) В регистър „Клиенти“ се съхраняват лични данни на физическите лица, с които дружеството сключва граждански договори за почистване на заявени от тях помещения.

(2) Данните, които се събират от субектите са следните: три имена, единен граждански номер (ЕГН), адрес, телефон за връзка, имейл адрес, банкови данни.

(3) Срокът, за който се съхраняват личните данни в регистър „Клиенти“ е 6 години от датата на прекратяване на договора.

Чл. 13. (1) В регистър „Контрагенти“ се съхраняват данните на субектите, с които дружеството сключва граждански договори, различни от договорите, които се сключват със субектите от регистър „Клиенти“.

(2) Данните, които се събират по този регистър са име и фамилия, адрес, телефон за връзка, имейл адрес, ако е наличен.

(3) Данните се съхраняват за срок от 6 години от датата на прекратяване на договора.

Глава трета **ВИДОВЕ ЗАЩИТА**

Чл.14. (1) Видовете защита на личните данни, прилагани при Администратора са:

- Физическа.
- Персонална.
- Документална.

Чл.15. (1) Физическата защита на личните данни представлява система от технически и организационни мерки за предотвратяване на нерегламентиран достъп до сгради, помещения и съоръжения, в които се обработват лични данни.

(2) Основните организационни мерки на физическата защита са:

1. Определяне на помещенията, в които ще се обработват лични данни.
2. Определяне на организацията на физическия достъп.
3. Определяне на използваните технически средства за физическа защита.
4. Определяне на екип за реагиране при нарушения.

(3) Основните технически мерки на физическата защита са:

1. Ключалки.
2. Шкафове.
3. Метални каси.
6. Охрана и/или система за сигурност, включително СОТ.
7. Пожарогасителни средства.
8. Пожароизвестителни и пожарогасителни системи.

Чл.16. (1) Персоналната защита представлява система от организационни мерки спрямо физическите лица, които обработват лични данни по указание на администратора.

(2) Основните мерки на персоналната защита са:

1. Познаване на нормативната уредба в областта на защитата на личните данни.

2. Познаване на настоящите вътрешни правила за защита на личните данни.
3. Знания за опасностите за личните данни, обработвани от администратора.
4. Споделяне на критична информация между персонала (например идентификатори, пароли за достъп и т.н.).
5. Съгласие за поемане на задължение за неразпространение на личните данни.
6. Обучение.
7. Тренировка на персонала за реакция при събития, застрашаващи сигурността на данните.

(3) Мерките за персонална защита гарантират достъпа до лични данни само на лица, чиито служебни задължения или конкретно възложена задача налагат такъв достъп.

(4) Лицата могат да започнат да обработват лични данни след запознаване със:

1. Нормативната уредба в областта на защитата на личните данни.
2. Настоящите вътрешни правила на личните данни.
3. Опасностите за личните данни, обработвани от администратора.

(5) При постъпване на работа лицата подписват декларация за неразгласяване на лични данни, до които са получили достъп при и по повод изпълнение на задълженията си.

Чл.17. (1) Документалната защита представлява система от организационни мерки при обработването на лични данни на хартиен носител.

(2) Основните мерки на документалната защита са:

1. Определяне на регистрите, които ще се поддържат на хартиен носител.
2. Определяне на условията за обработване на лични данни.
4. Определяне на срокове за съхранение.
5. Процедури за унищожаване.
6. Процедури за проверка и контрол на обработването.

Глава четвърта

ФОРМИ НА СЪХРАНЕНИЕ НА ЛИЧНИТЕ ДАННИ

Раздел 1

Лични данни на хартиен носител

Чл.18. Форма на организация и съхраняване на личните данни на хартиен носител:

1. Папките, съдържащи лични данни, са разположени в шкафове в офис пространството, което се заключва.
2. Лични данни на хартиен носител се обработват в офис пространството, от служителите, които сключват договор със субекта на данни.
3. Носител (форма) за предоставяне на данните от физическите лица - личните данни за всяко лице се набират с цел и в изпълнение на сключения със субекта договор:

- устно интервю с лицето;
- хартиен носител - писмени документи (заявления, запитвания) по текущи въпроси в процеса на работа, подадени от лицето;

4. Възможността за предоставяне другиму достъп до личните данни при обработката им е ограничена и се извършва само в хипотезите и при условията, изрично предвидени в Общия регламент за защита на личните данни.

Раздел 2

Лични данни на технически носител

Чл.19. Форма на организация и съхраняване на личните данни на технически носител:

1. Личните данни се въвеждат на твърд диск на сървър от компютърната мрежа (в случай, че се обработват от повече от един служител. Компютрите са свързани в локалната мрежа, като всяко от компютърните устройства има достъп до интернет. Наличен е безжичен интернет (wi-fi), като достъпът е защитен с парола, която е известна единствено на служителите на дружеството.

2. При работа с данните се използват съответните софтуерни продукти за обработка, като вътрешна система за управление на клиентите. Данните се въвеждат в компютъра от хартиен носител и при контакт с клиентите.

3. Достъп до файловете за обработка на лични данни имат само работещите с тях. Носители с лични данни могат да се разпространяват само ако е използван механизъм, гарантиращ, че данните не могат да се четат или променят при пренасянето им.

4. Забранено е използването на преносими лични носители на данни в звената, в които се обработват лични данни.

5. Работните компютърни конфигурации, както и цялата ИТ инфраструктура, включително и достъпът до интернет, се използват единствено за служебни цели.

6. При ремонт на компютърна техника, на която се съхраняват лични данни, предоставянето ѝ на сервизната организация се извършва без устройствата, на които се съхраняват лични данни.

Глава пета

ЗАДЪЛЖЕНИЯ НА АДМИНИСТРАТОРА

Чл. 20. Администраторът има следните задължения:

1. Определя политиката за защита на личните данни в дружеството.
2. Осигурява организацията по водене на регистрите.
3. Прилага конкретни мерки за защита съобразно спецификата на водените регистри.
4. Осъществява контрол по спазване на изискванията за защита на регистрите, установява обстоятелства, свързани с нарушаване на тяхната защита, и предприема мерки за тяхното отстраняване.
5. Актуализира поддържаните регистри с лични данни.
6. Оказва съдействие при осъществяване на контролните функции на Комисията

за защита на личните данни.

Глава шеста

ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§1. Настоящите вътрешни правила за дейността на „БИЗНЕС КАТАЛОГ“ ЕООД по защита на личните данни са приети от Единоличния собственик на капитала на 25.05.2018 г.