ДОГОВОР ЗА ОБРАБОТКА НА ДАННИ

*Като се има предвид, че:*

„Йелоу 333” АД, с ЕИК [175206481](https://public.brra.bg/CheckUps/Verifications/ActiveCondition.ra?guid=b501948844fc46bda55e7b146c0bd4e8), със седалище и адрес на управление: гр. София 1172, район Изгрев, бул. „Никола Габровски” № 1 („**Обработващ**”) и

……………………………………………., ЕИК …………………………, със седалище и адрес на управление: ………………………………… („**Администратор**”) са сключили Абонаментен договор за предоставяне на транспортни услуги от дата\_\_\_\_\_\_\_\_\_\_\_\_ ("**Основен договор**"),

*Като се има предвид*, че във връзка с Основния договор Обработващият обработва определени лични данни от името и за сметка на Администратора,

*Като се има предвид*, че Обработващият и Администратора са длъжни да определят целите на обработване на личните данни и да спазват Действащото Законодателство в областта на личните данни (както е дефинирано по-долу),

Обработващият и Администратора (по-надолу заедно и "**Страните**") сключват този договор на \_\_\_\_\_\_\_\_\_\_\_\_ 2018 г.

Чл. 1. **Определения**

|  |  |
| --- | --- |
| Действащо Законодателство в областта на личните данни | означава всеки действащ (сега или в бъдеще) законов и/или подзаконов (нормативен или ненормативен (общ или индивидуален административен)) акт (включително GDPR), който се отнася до защитата на личните данни на физическите лица и правомерното обработване на такива лични данни; |
| GDPR | Означава Общ регламент за защита на личните данни или Регламент (EU) 2016/679, съгласно който Директива 95/46/EC за защита на лица по отношение на обработка на лични данни и свободното движение на такива данни се отменя (и съответно всички позовавания в този Договор на Действащото Законодателство в областта на личните данни ще се тълкуват в съответствие с GDPR към датата на неговото приложение – 25 май 2018 г.); |
| Лични данни | означава каквато и да е информация отнасяща се до физическо лице, както е определена по Действащото Законодателство в областта на личните данни и включваща категориите данни описани в Приложение 1 към този договор.) заедно с допълнителни лични данни, до които Обработващият може да има достъп към всеки един момент при изпълнение на този договор и Основния договор; |
| КЗЛД | означава Комисия за защита на личните данни на Република България; |
| Обработка | означава каквото и да е действие или поредица от действия, които се извършват с Лични данни, включително и не само събиране, структуриране, съхранение, адаптиране или промяна, извличане, използване, разкриване чрез предаване, разпространение или предоставяне по друг начин, изтриване или унищожаване на Лични данни, както е предвидено от Действащото Законодателство в областта на личните данни; |
| Технически и организационни мерки | означава техническите и организационни мерки за сигурност, определени в Приложение 2 към този договор, които могат да бъдат актуализирани към който и да е момент от Администратора в съответствие с условията на този договор. |

Чл. 2. **Цели и предмет на Обработката. Видове данни.**

(1) Администраторът определя целите и предмета на Обработка, както и видовете данни, които Обработващият обработва от името на Администратора във връзка с правата и задълженията на Страните по Основния договор. Целите и предмета на Обработката, както и категориите и отделните видове данни са описани в Приложение 1 към този договор.

(2) Обработващият извършва Обработка на Лични данни единствено по изрично и документирано указание на Администратора. В случай, че Обработващият предприема действия по обработка на данни по този договор или по Основния договор без това да е съгласувано с Администратора и без да е получил документирано указание за това, то за тези действия Обработващия ще носи отговорност като администратор на лични данни по смисъла на Действащото Законодателство в областта на личните данни.

(3) Всички видове указания на Администратора по този договор се документират и предават на Обработващия в писмена форма (например електронна).

Чл. 3. **Отговорности**

(1) Обработващият и Администраторът спазват Действащото Законодателство в областта на личните данни и изпълняват задълженията си по този договор по начин, че да не нарушават което и да е от законовите си задължения.

(2) Администраторът носи отговорност за всички свои указания към Обработващия и спазването на определените от него цели и предмет на Обработката, както и за осигуряване правата на субектите на Лични данни.

(3) Преди започване на Обработката и по всяко време след това Обработващият незабавно уведомява Администратора, ако, до колкото му е известно, което и да е документирано указание на Администратора нарушава Действащото Законодателство в областта на личните данни.

Чл. 4. **Срок на Обработката**

(1) Срокът на Обработката по този договор, съвпада със срока на действие на Основния договор, освен ако целите на обработка на данните не се изпълнят по някаква причина и по-рано. След този срок могат да се обработват единствено Личните данни, които следва да се съхраняват и след този срок на законово основание и/или по изрично указание на Администратора, при спазване на Действащото Законодателство в областта на личните данни.

(2) Всички срокове по този член се описват изчерпателно в Приложение 1 към този договор.

Чл. 5. **Сигурност на информацията**

Обработващият гарантира, че поддържа и ще продължи да поддържа подходящи и достатъчни Технически и организационни мерки за сигурност (както са описани в Приложение 2 към този договор), за да предпази Личните данни от случайно или незаконосъобразно унищожаване или случайна загуба, или достъп до тях.

Чл. 6. **Обработка на Лични данни**

Обработващият гарантира по отношение на Личните данни, които обработва от името на Администратора, че:

а. извършва Обработка само за целите, определени в Приложение 1, като в процеса на Обработка действа единствено съгласно документираните указания на Администратора, включително такива указания да спре по-нататъшна Обработка;

б. не упражнява самостоятелно контрол върху Личните данни;

в. не прехвърля Лични данни на трети лица, освен ако друго не е изрично указано от Администратора.

Чл. 7. **Съдействие и право на одит**

(1) Обработващият оказва съдействие на и подпомага доколкото му е възможно Администратора, включително и не само като му предоставя всякаква информация, която Администраторът може основателно да поиска, за да е в състояние да изпълни задълженията си по Действащото Законодателство в областта на личните данни или по предписание на КЗЛД по отношение на Личните данни, които са обект на Обработка по този договор, както и задълженията на Администратора по отношение на отделните субекти на Лични данни.

(2) Във връзка с ал. 1 на този член Обработващият позволява на Администратора и допринася за извършването на одити, включително проверки, от страна на Администратора или друг одитор, оправомощен от Администратора с цел доказване от страна на Обработващия на начина, по който извършва Обработката и Техническите и организационни мерки, които предприема. Одитиращата страна понася разноските си във връзка с одита.

(3) Доказателство за спазването на задълженията на Обработващия може да бъде предоставено чрез:

а. Спазване на одобрените Кодекси за поведение, съгласно член 40 от GDPR (ако такива са налични);

б. Сертифициране, съгласно одобрена процедура за сертифициране, в съответствие с член 42 от GDPR;

в. Съобразяването със стандартни договорни клаузи, съгласно член 28 (6) от GDPR;

г. Удостоверяване от одитор; доклади или извадки от доклади, предоставени от независими органи (напр. одитор, Длъжностно лице по защита на данните, отдел за информационна сигурност, одитор за поверителност на данни, одитор за качество и др.)

д. Подходящо удостоверяване от информационна сигурност или одит за защита на данни (напр. [ISO/IEC 27001](https://de.wikipedia.org/wiki/ISO/IEC_27001)).

Чл. 8. **Искания от трети лица**

(1) Ако не е забранено от Действащото Законодателство в областта на личните данни, Обработващият уведомява своевременно Администратора за всяко искане, съобщение, молба, претенция или оплакване отправени директно към него от:

а. който и да е държавен, регулаторен, съдебен, надзорен орган, включително КЗЛД; и/или

б. който и да е субект на Лични данни;

(2) Обработващият оказва разумно съдействие на Администратора, за да може Администратора да отговори на нуждите на лицата по ал 1 от този член.

(3) Обработващият не разкрива и няма задължение да разкрива директно Лични данни към каквито и да е физически или юридически лица, освен ако такова разкриване не е задължително по силата на Действащото Законодателство в областта на личните данни.

Чл. 9. **Длъжностно лице по защита на данните**

Обработващият и Администраторът спазват правните изисквания за назначаване на длъжностно лице по защита на данни, съгласно член 37 GDPR, ако се окаже, че такова е задължително необходимо.

Чл. 10. **Трансфер на Лични данни в трети държави**

Обработката на Лични данни по този договор няма да включва трансфер на Лични данни в трети държави, по смисъла на Действащото Законодателство в областта на личните данни.

Чл. 11. **Нарушение на сигурността на Личните данни и изисквания за уведомяване**

(1) Обработващият информира Администратора без ненужно забавяне и по възможност в рамките на 48 часа за каквото и да е случайно, непозволено или незаконно унищожаване, загуба, промяна или разкриване на или достъп до Лични данни ("**Нарушение на сигурността**").

(2) Такова уведомление включва всички елементи определени в член 33, ал 3 на GDPR и в допълнение каквато и да е друга информация, която Обработващия прецени, че е необходима във връзка с Нарушението на сигурността, веднага след като такава информация може да бъде събрана или стане достъпна за Обработващия.

(3) След консултация с Администратора, Обработващият предприема незабавни действия за разследване и отстраняване на Нарушението на сигурността с цел да установи, предотврати и положи всички усилия за да намали ефекта от такова Нарушение на сигурността.

Чл. 12. **Поверителност**

(1) Всяка информация от какъвто и да е вид (независимо дали е техническа, търговска, финансова, оперативна или друга) и под каквато и да е форма (устна, писмена, записана или друга), включително Лични данни станала известна на Обработващия и Администратора по отношение на или в резултат на този договор, се считат за поверителни. Данни, свързани с базата данни, вътрешните правила и процедурите на Обработващия, се считат също за поверителна информация.

(2) Обработващият ще осигури надеждността на всички свои служители, които имат достъп до Личните данни по този договор и запознаването им с вътрешните правила за поверителност на Обработващия във връзка с Обработката на Лични данни.

Чл. 13. **Под-обработващи**

(1) За целите на настоящия договор за под-обработване следва да се разбира всяка Обработка, която е пряко свързана с Обработката по този договор и с нуждите по Основния договор, но не се извършват директно от Обработващия.

(2) Обработващият не включва Под-обработващ данни без предварителното конкретно писмено разрешение на Администратора. Обработващият данни винаги информира Администратора за всякакви планирани промени за включване или замяна на Под-обработващи.

(3) В случай на използване на под-обработващи, Обработващият изисква от тях да спазват разпоредбите на този договор и гарантира, че Администраторът може също така да упражни своите права, произтичащи от този договор (по-специално правото му да извършва инспекции и контрол) директно върху такива под-обработващи.

(4) В случай, че е планирано използване на под-обработващи от трета държава (извън ЕС и/или ЕИП), Обработващият гарантира, че съответните под-обработващи поддържат подходящо ниво на защита на данните (например чрез сключване на споразумение, основано на стандартните договорни клаузи на ЕС). Обработващият ще предостави на Администратора доказателства за съществуването на такива споразумения с под-обработващите по искане на Администратора.

Чл. 14. **Изтриване на Лични данни**

(1) По избор на Администратора Обработващият заличава или връща на Администратора всички Лични данни след приключване на Обработката, съгласно Срока за Обработка чл. 4 от този договор или прекратяването на този договор при условията на чл. 15 тук по-долу, и заличава съществуващите копия, освен ако Действащото Законодателство в областта на личните данни не изисква тяхното съхранение.

(2) Отделно от ал. 1 на този член, по всяко време през срока на договора Обработващият няма право да изтрива и/или запазва Лични данни без изричното документирано указание на Администратора за това.

Чл. 15. **Срок и прекратяване**

Настоящият Договор влиза в сила при подписването му от двете Страни и действа до настъпване на едно от следните събития: (а) изтичане на срока по Основния договор (респ. Срока на Обработка по този договор); (б) прекратяването на Основния договор.

Чл. 16. **Невалидност**

Невалидността на някой термин, условие или клауза от този договор не може да повлияе на валидността на останалите клаузи на договора или на валидността на самия договор.

Чл. 17. **Уведомления и документирани указания**

Всички уведомления между Страните, както и документираните указания на Администратора към Обработващия по този договор ще се извършват в писмена форма на адресите и лицата за контакт посочени по-долу (като всяка промяна в тях, следва да бъде съобщена в писмена форма):

За „Йелоу 333” АД За ………………………..

Лице за контакт: Лице за контакт:

Адрес: гр. София, бул. „Н. Габровски” № 1 Адрес:

Ел.Поща: [s.kukeva@yellow333.com](mailto:s.kukeva@yellow333.com) Ел.Поща:

Чл. 18. **Приложимо Право**. **Спорове.**

Приложимото за този договор право е българското. Всички спорове между Страните произтичащи от и/или свързани с този договор ще се разрешават от компетентния за това съд в гр. София.

Чл. 19. **Заглавия.**

Заглавията на членовете в този договор служат за удобство и не представляват част от този договор.

За Обработващия: За Администратора:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Приложение А

към договор за обработка на данни сключен на \_\_\_\_\_\_\_\_\_\_\_ 2018 между Обработващия и Администратора […]

1. Описание на Услугите (по смисъла на чл. 1 и съгласно Основния договор)

2. Естество и цел на планираната Обработка на данни

Целите и предмета на Обработката на Лични данни са описани в Основния договор, а именно …………………………………….

3. Видове Данни

Предметът на Обработката на Лични данни се състои от следните видове данни:

☐ Биометрични данни – видео изображения, снимки и др.

☐ Глас

☐ Имена

☐ Адреси (пощенски, имейл, IP и др)

☐ Дата и място на раждане

☐ Трафични и подобни телеком данни

☐ Телефонни номера

☐ Данни, събирани въз основа на договор

☐ Данни, които определят локацията на субекта на Лични данни (GPS позиция)

☐ Данни, които определят локацията на притежавани от субектите на Лични данни МПС

☐ Данни за използването на притежавани от субектите на Лични данни МПС, като: изминатото разстояние, продължителността на шофиране; скорост на превозното средство, продължителност на пътуването и разстояние; регистрационни данни и др.)

☐ Други (Моля, опишете):…………………………………..

4. Категории Субекти на Лични данни

☐ Клиенти

☐ Потенциални клиенти

☐ Абонати

☐ Служители

☐ Доставчици

☐ Оторизирани представители

☐ Лица за контакт

☐ Други (Моля, посочете): …………………………………

5. Срок на Обработка: документите (електронни и на хартия) се пазят съгласно изискванията на българското законодателство.

Приложение Б

към договор за обработка на данни сключен на \_\_\_\_\_\_\_\_\_\_\_ 2018 между Обработващия и Администратора

**ТЕХНИЧЕСКИ И ОРГАНИЗАЦИОННИ МЕРКИ ЗА СИГУРНОСТ НА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ**

1. **Задължения на Обработващия**
   1. Обработващият се задължава:
      1. да предотвратява неоторизиран достъп на лица без разрешение до личните данни и до начините на тяхното обработване;
      2. да предотвратява всяко неразрешено гледане, създаване, копиране, прехвърляне, промяна или изтриване на записи/файлове, съдържащи лични данни;
      3. да приема мерки, които му позволяват да идентифицира и проверява на кого са прехвърлени лични данни; и
      4. да приема политики, уреждащи правилата за достъп и по-нататъшна обработка на личните данни.
   2. По отношение автоматичното обработване на лични данни, ако е приложимо, във връзка с обработката на данни, които се извършват съгласно Договора, Обработващият:
      1. да определи помещения, които да се разположат елементите на комуникационно-информационните системи за обработване на личните данни;
      2. гарантира, че системите за автоматично обработване на лични данни се използват само от упълномощени лица;
      3. гарантират, че лицата, оправомощени да използват системи за автоматично обработване на лични данни, имат достъп само до личните данни, съответстващи на тяхното овластяване и въз основа на конкретни разрешения, дадени нарочно за тези лица;
      4. предотвратява неоторизиран достъп до носители на данни.
2. **Специални мерки на Обработващия за защита на личните данни**
   1. *Физически достъп*

Обработващият поддържа физически стандарти за сигурност, предназначени да забранят и недопуснат неоторизиран физически достъп до помещенията и оборудването на Обработващия, в което се извършва обработката на данните, предмет на Основния договор.

* + 1. определяне на помещенията, в които ще обработват личните данни;
    2. определя и въвежда контрол на зоните за сигурност чрез подходящ контрол за влизане, за да се гарантира че достъп имат само оторизирани лица;
    3. Обработващият определя организацията на физическия достъп, включително като определя физическия достъп до помещенията, в които ще се обработват личните данни, да бъде ограничен до служители и изпълнители/подизпълнители на Обработващия и други, овластени от него лица;
    4. видеонаблюдение на достъпа до помещенията на Обработващия, включително на забранените зони и оборудването в помещенията;
  1. *Контрол и администриране на достъпа*

Обработващият поддържа следните правила, политики, стандарти и процедури за контрол на достъпа и администриране на съответната ИТ среда, ако е приложимо, във връзка с обработката на данни, които се извършват съгласно Договора:

* + 1. приема се политика за контрол на достъпа, която документира подходящи практики в областта на търговската и информационната сигурност, която политика следва да включва и следното: поставяне на ключалки на шкафове и сейфове, в които се съхраняват на хартия лични данни, поставяне и осигуряване функционирането на пожарогасителни средства;
    2. приемане на формален процес на регистрация и дерегистрация на потребители, който се прилага с оглед възлагането на права за достъп;
    3. приемане на формален процес за достъп на потребители, който се прилага при възлагане или оттегляне на права за достъп за всички видове потребители до всички видове системи и услуги;
    4. формален процес за управление и контролирано предоставяне на информация за тайна идентификация;
    5. правата за достъп на потребителите се преразглеждат на редовни интервали от време;
    6. достъпът до системи и приложения за обработване на лични данни се контролира чрез подходяща и сигурна процедура за регистрация и вписване;
    7. администраторските профили следва да се използват само за целта за изпълнение на административни дейности;
    8. достъпът до компютри и сървъри трябва да бъде според и в съответствие с обхвата на длъжността и функциите на служителя или изпълнителя.
  1. *Персонал на Обработващия*
     1. Служителите и изпълнителите/подизпълнителите са получили адекватно и подходящо обучение по политиките за защита и сигурност на Обработващия и са наясно със своите отговорности по отношение поверителността, защитата и сигурността на личните данни. Налице са адекватни и подходящи процедури и политики за продължаване на обучението на всички служители и изпълнители/подизпълнители, включително всички допълнителни служители и изпълнители, които предоставят услуги на Обработващия.
     2. Служителите на Обработващия и одобрените от Администратора изпълнители/подизпълнители, са задължени да пазят поверителността на личните данни и конфиденциалната информация на Администратора и да спазват приложимите правила, стандарти или изисквания на Обработващия във връзка с обработването на личните данни на Администратора.
  2. *Непрекъсваемост и възстановяване на работния процес*

Обработващият има възможност да възстанови своевременно наличността и достъпа до личните данни в случай на физически или технически инцидент:

* + 1. за всички системи, обработващи лични данни, са установени изисквания за непрекъсваемост на работата и са изготвени и тествани планове за възстановяване след инцидент; и
  1. *Уведомяване за нарушаване на сигурността и управление на инциденти*

Страните взаимно следва да се уведомят в случай на инцидент, свързан със сигурността, който засяга Услугите по Основния договор, като уведомленията за това се изпращат на имейлите, посочени по-горе във възможно най-кратки разумни срокове.