

ТОБО ООД
ПОЛИТИКА И ВЪТРЕШНО-ФИРМЕНИ ПРАВИЛА
ИНСТРУКЦИЯ
ЗА МЕХАНИЗМА НА ОБРАБОТВАНЕ И ЗАЩИТА НА ЛИЧНИ ДАННИ

I. ОСНОВАНИЕ

Чл. 1.(1) Настоящите правила са изготвени в съответствие с изискванията на Регламент (ЕС) 2016/679 на Европейския Парламент и на Съвета от 27 април 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 (Общ регламент относно защитата на данните).

(2) Настоящите правила определят реда, по който ТОБО ООД с ЕИК 831301080 („Дружеството“) събира, записва, организира, структурира, съхранява, адаптира или променя, извлича, консултира, използва, разкрива чрез предаване, разпространяване или друг начин, по който данните стават достъпни, подрежда или комбинира, ограничава, изтрива, унищожават или обработва по друг начин лични данни за целите на своята дейност.

(3) В зависимост от конкретната ситуация, Дружеството може да обработва данни в качеството на администратор или обработващ.

II. ЦЕЛИ И ОБХВАТ НА ИНСТРУКЦИЯТА

Чл. 2. Цели -Настоящите правила имат за цел да регламентират:

(1) Целия процес по обработване на личните данни -Принципите, процедурите и механизмите за обработка на личните данни: събиране, основанийето за обработка и съхранение тези данни ; формите за обработване на тези лични данни-регистри, сроковете за съхранение

(2) Сроковете за съхранение

При съхранението на данни, Ние прилагаме генералния принцип за съхранение на данни в минимален обем и за срок не по-дълъг от необходимото.

Сроковете за необходимостта от съхранение се определят от различни нормативни актове в областта на трудовото законодателство и други специфични законови изисквания (пример- ЗУТ- гаранционните срокове за строителните обекти и др.) За част от документите подходящият срок за съхранение се определя по преценка на Администратора-в случая-Работодателя.

(3)Лицата, които обработват лични данни, и техните задължения;

(4)Процедурите за уведомяване на надзорния орган в случай на нарушения в сигурността;

(5)Процедурите за администриране на искания за достъп до данни, коригиране на обработваните данни, възражения и оттегляне на съгласия, както и администриране на искания за упражняване на други права, които субектите на лични данни имат по закон;

(6)Правилата за предаване на лични данни на трети лица в България и чужбина;

(7)Техническите ресурси, прилагани при обработката на лични данни и необходимите **технически и организационни мерки за защита** на личните данни на посочените по-горе лица от неправомерно обработване (случайно или незаконно разрушаване, случайна загуба или промяна, незаконно разкриване или достъп,

нерегламентирано изменение или разпространение, както и от всички други незаконни форми на обработване на лични данни).

(8)Механизмите за контрол за сигурност на личните данни и минимизиране на риска от загубата им , или злоупотребата с тях.

Чл. 3. Обхват: Инструкцията/правилата са задължителни за целия персонал, имащ достъп до лични данни в регистрите .

III. СУБЕКТИ НА ДАННИ И КАТЕГОРИИ ЛИЧНИ ДАННИ

Чл. 4. (1) Дружеството събира и обработва лични данни, необходими за осъществяване на своите права и задължения като работодател, доставчик на услуги и контрагент при съблюдаване изискванията на приложимото законодателство. Личните данни, обработвани от Дружеството, са групирани в регистри на дейностите по обработване, съдържащи правила за обработване на лични данни, отнасящи се до:

- работници и служители и изпълнители по граждански договори;
- кандидати за работа;
- клиенти;
- доставчици на услуги.

(2) Относно лицата, заети по трудови или граждански правоотношения в дружеството, и на кандидатите за работа, се събират следните лични данни:

а) Идентификация: име; ЕГН (дата на раждане), постоянен и/или настоящ адрес, телефон, данни по лична карта или паспортни данни;

б) Образование и професионална квалификация; данни, свързани с образование, трудов опит, професионална и лична квалификация и умения;

в) Здравни данни: здравословно състояние, ТЕЛК решения, медицински свидетелства, болнични листове и всяка прилежаща към тях документация;

г) Други данни: свидетелство за съдимост, когато се изисква представянето му съгласно нормативен акт, както и други данни, чието обработване е необходимо за изпълнение на правата и задълженията на Дружеството като работодател.

(3) Относно физически лица, клиенти на дружеството, се събират лични данни, които са необходими за изпълнението на законовите задължения на дружеството като доставчик на услуги, както следва:

- име; ЕГН (дата на раждане), постоянен и/или настоящ адрес, телефон, данни по лична карта или паспортни данни.

(4) Относно физически лица, доставчици на услуги на дружеството, се съхраняват лични данни, необходими за сключването и изпълнението на договори за предоставяне на услуги на дружеството от външни доставчици, както следва:

- име, ЕГН (дата на раждане), постоянен и/или настоящ адрес, телефон, данни по лична карта или паспортни данни; електронна поща.

(5) Дружеството обработва чувствителни данни, само доколкото това е необходимо за изпълнение на специфичните му права и задължения в областта на трудовото и осигурително законодателство.

IV. ЦЕЛИ И ПРИНЦИПИ НА ОБРАБОТВАНЕ НА ЛИЧНИТЕ ДАННИ

Чл. 5.Цели на обработването на лични данни: конкретни, изрични легитимни

ТОБО ООД събира, използва и обработва информацията за целите, посочени в Общия РЕГЛАМЕНТ EU 2016/679-и предвидени в настоящата Политика , които могат да бъдат:

-Цели, необходими за изпълнението на законови задължения на ТОБО ООД

-Цели, необходими за сключването и изпълнението на договор

-Цели, необходими за защита и прилагане на легитимните интереси на други ползватели на Услугите, трети лица и ТОБО ООД;

-Цели, за които има дадено изрично съгласие;

- (1) управление на човешките ресурси, изплащане на трудовите възнаграждения и изпълнение на свързаните с това задължения на работодателя за удържане и плащане на здравни и социални осигуровки на служителите, на данъци, както и на други права и задължения на Дружеството в качеството му на работодател;
- (2) администриране на отношенията с клиенти на дружеството и предоставяне на услуги;
- (3) сключване и изпълнение на договори с доставчици за предоставяне на услуги на Дружеството.

Чл. 6. Личните данни се обработват законосъобразно, добросъвестно и прозрачно при спазване на следните принципи:

- (1) Субектът на данните се информира предварително за обработването на неговите лични данни;
- (2) Личните данни се събират за конкретни, точно определени и законни цели и не се обработват допълнително по начин, несъвместим с тези цели;
- (3) Личните данни съответстват на целите, за които се събират;
- (4) Личните данни трябва да са точни и при необходимост да се актуализират;
- (5) Личните данни се заличават или коригират, когато се установи, че са неточни или не съответстват на целите, за които се обработват;
- (6) Личните данни се поддържат във вид, който позволява идентифициране на съответните физически лица за период, не по-дълъг от необходимия, за целите, за които тези данни се обработват.

Чл. 7. За да е законосъобразно обработването на данните, трябва да е налице поне едно от следните условия:

- (1) Субектът на данните е дал своето съгласие;
- (2) Обработването е необходимо за изпълнението на договор, по който субектът на данните е страна, или за предприемане на стъпки по искане на субекта на данните преди сключването на договор;
- (3) Обработването е необходимо за спазването на законово задължение, което се прилага спрямо администратора;
- (5) Обработването е необходимо за изпълнение на задача от обществен интерес;
- (6) Обработването е необходимо за целите на легитимните интереси на администратора, освен когато пред тези интереси преимущество имат интересите или основните права и свободи на субекта на данни. В този случай, целите, за които се обработват лични данни на това основание, са описани в приложимите известия по защита на данните.

Чл. 8. Съгласие

(1) Субектът на данни е съгласен с обработването, ако изрази това ясно и недвусмислено – чрез изявление или друг потвърждаващ акт. Ако съгласието за обработка на лични данни се дава чрез документ, който урежда и други въпроси, то следва да бъде изискано отделно от съгласието по други въпроси.

(2) Личните данни се набират в изпълнение на нормативно задължение на ТОВО-при постъпване на дадено лице на работа в ТОВО, при заявка за закупуване на имот, или възлагане на поръчка, или друго законово основание.

(3) Във всички случаи, когато Администраторът ТОВО събира лични данни, лицето, което ги предоставя, подписва документ (**декларация за съгласие**), в който дава изричното си съгласие, данните му да бъдат обработвани и съхранявани. **При наличие на законово основание за обработка**, лицето подписва **Уведомление**.

(4) „Съгласието“ (Уведомлението) се подписва в два екземпляра, задължително съдържа данни по личната карта на лицето, основанието за обработка и съхранение, имената на служителя, „обработващ лични данни“ и текст за конфиденциалност.

Съдържа също така и текст за правата на субекта на данните, а именно : за промяна на данните от собственика им, правото му на достъп до данните по всяко време, правото да бъдат заличени данните, в случай, че това не противоречи на законово определения срок за съхранението им.

(5) Субектите на данни трябва да могат лесно да оттеглят съгласието си за обработване по всяко време, и оттеглянето трябва да бъде уважено своевременно. Ако не съществува друго условие за законосъобразност на обработването, с оттеглянето на съгласието то следва да се прекрати.

(6) Декларациите за съгласие се съхраняват от дружеството, докато се извършват действия по обработване на данни на това основание, с оглед спазването на принципа на отчетност.

V. ПРОЦЕДУРИ ПО ОБРАБОТВАНЕ НА ЛИЧНИТЕ ДАННИ

Чл. 9. Процедура за обработване на личните данни, отнасящи се до лицата, заети по трудови или граждански правоотношения в дружеството, както и на кандидатите за работа

(1) Личните данни, отнасящи се до лицата, заети по трудови или граждански правоотношения в Дружеството, както и на кандидатите за работа, се събират при и по повод набирането на персонал. Данните на всеки работник и служител на Дружеството се съхраняват в лични досиета, като някои данни могат да се съхраняват или обработват и на технически носител.

Данните на кандидатите за работа, от проведени конкурси и интервюта, се съхраняват на хартиен носител само докато се проведе интервюто, след което информацията се унищожават.

(2) Личните досиета се подреждат в специални картотечни шкафове (заклучени), находящи се в помещението на Счетоводителя (Човешки ресурси), отговарящ за личните данни.. Достъпът до кабинета се предоставя само на лицата, оправомощени да обработват личните данни, като за целта се създава специален ред за влизане в помещението чрез ключ.

(3) Лицата, оправомощени да обработват лични данни, предприемат всички организационно-технически мерки за съхраняването и опазването на личните досиета и класъорите с информация, в това число ограничаване на достъпа до тях на външни лица и неоторизирани служители.

(4) Досиета на работниците и служителите, както и данните на кандидатите за работа, не се изнасят извън сградата на дружеството.

Чл. 10. Процедура за обработване на лични данни, отнасящи се до контрагенти, партньори, възложители , подизпълнители и доставчици на услуги

(1) Личните данни, отнасящи се до горепосочената категория субекти, се събират при подаване на заявка за предоставяне на услуга или сключване на договор с Дружеството.

(2) Личните данни, отнасящи се до доставчици на услуги, се събират при сключване на договор с доставчик на услуги, като обичайно личните данни се съдържат в текста на самите договори.

(3) Личните данни се съхраняват на електронен и хартиен носител (подписани копия на сключените договори), които се класират в отделни досиета. Досиетата се съхраняват в шкафове, които се заключват, в кабинета на Лицето, отговорно за личните данни. Електронните данни се съхраняват в бази данни.

Чл. 11. Процедура за обработване на лични данни, отнасящи се до клиенти на недвижими имоти-за осъществяване на проектантската, строителната и търговска дейност на Дружеството

(1) Личните данни, отнасящи се до клиенти, се събират при подаване на заявка за предоставяне на услуга или сключване на договор с клиент на Дружеството

VI. ДОКУМЕНТИРАНЕ НА ОБРАБОТКАТА НА ЛИЧНИ ДАННИ

Чл. 12. (1) Дружеството документира дейностите по обработване на лични данни при спазване на принципа на отчетност.

(2) Документацията трябва да е достатъчна, за да докаже спазването на принципите за законосъобразно обработване на личните данни.

(3) Обработването на данни, свързано с предаване на данни на обработващи, установени в страната или чужбина; съхранение на данни на сървъри, собственост на трети лица; архивиране или изтриване на данни; въвеждане на псевдонимизация, както и всяка друга обработка, чиито параметри са различни от описаните в тези правила, се документира чрез създаване на протоколи, които съдържат следната информация:

(а) целите на обработването;

(б) категориите лични данни и категориите субекти на данни;

(в) категориите получатели, пред които са или ще бъдат разкрити личните данни, включително получателите в трети държави;

(г) предаването на лични данни на трета държава;

(д) когато е възможно, предвидените срокове за изтриване на различните категории данни;

(е) общо описание на техническите и организационни мерки за сигурност.

(4) Протоколите се изготвят от лицата, които извършват съответната обработка на данни по указания от Лицето, отговорно за личните данни.

(5) Съвкупността от всички протоколи, съдържащи гореописаната информация, съставлява регистъра на дейностите по обработването, съгласно чл. 30 от ОРЗД.

Чл.13. Регистри-Видове и предназначение:

Видовете регистри отразяват реалните информационни потоци (лични данни) в различните отдели (звена) на Дружеството.

ТОБО като администратор на лични данни, поддържа регистри **с всички категории дейности по обработване на данните**, с определени за поддръжката им отговорни служители, т.н. **„обработващи лични данни“**.

(1). **Видовете регистри** на дейностите по обработване (чл.30), **в ТОБО :**

- **-Регистър „Финансово –счетоводен“ и Регистър „Човешки ресурси“**
- **-Регистър "Клиенти- проучване , проектиране, изграждане и продажба /наем на недвижими имоти"**
- **-Регистър "Възложители, контрагенти, партньори, доставчици, подизпълнители"(юридическилица и физически лица),**
- **-РЕГИСТЪР „ВИДЕОНАБЛЮДЕНИЕ“-**

- **-За ТОБО ХОТЕЛИ ООД :**
- **-Регистър „Финансово –счетоводен“ и Регистър „Човешки ресурси“**
- **-РЕГИСТРИ „ГОСТИ ХОТЕЛ“ (за ТОБО Хотели ООД)-хотел „Латинка“-София и хотел „ВЕЛЕКА“-Черноморец, община Созопол**
- **-РЕГИСТРИ „ВИДЕОНАБЛЮДЕНИЕ“ за ТОБО Хотели ООД; срок за съхранение -30дни**

РЕГИСТЪР „ФИНАНСОВО –СЧЕТОВОДЕН“ И РЕГИСТЪР „ЧОВЕШКИ РЕСУРСИ“-

(1) Регистърът набира и съхранява лични данни на служителите и изпълнителите по трудови и граждански договори в дружеството, по време на дейността им по изпълнение на тези договори с оглед:

1. индивидуализиране на трудовите и гражданските правоотношения;

2. изпълнение на нормативните изисквания на Кодекса на труда, Кодекса за социално осигуряване, Закона за счетоводството, Закона за държавния архив, Професионално осигуряване-Застрахователи и др.;

3. използване на събраните данни за съответните лица за служебни цели:

- за всички дейности, свързани със съществуване, изменение и прекратяване на трудовите и граждански правоотношения – за изготвяне на всякакви документи на лицата в тази връзка: договори, допълнителни споразумения, документи, удостоверяващи трудов стаж, служебни бележки, справки, удостоверения и др. подобни;
- за установяване на връзка с лицето по телефон, за изпращане на кореспонденция, отнасяща се до изпълнение на задълженията му по трудови или граждански договори;
- за водене на счетоводна отчетност относно възнагражденията на посочените по-горе лица по трудови и граждански договори;

РЕГИСТЪР " КЛИЕНТИ- ПРОУЧВАНЕ , ПРОЕКТИРАНЕ, ИЗГРАЖДАНЕ И ПРОДАЖБА /НАЕМ НА НЕДВИЖИМИ ИМОТИ"

Регистърът набира и съхранява лични данни на клиентите на дружеството с цел осъществяване на проектантската, строителната и търговска дейност на последното. Данните се събират при подаване на заявка за предоставяне на услуга, или сключване на договор с клиент на Дружеството.

РЕГИСТЪР "ВЪЗЛОЖИТЕЛИ, КОНТРАГЕНТИ, ПАРТНЬОРИ, ДОСТАВЧИЦИ, ПОДИЗПЪЛНИТЕЛИ" (ЛИЧНИ ДАННИ НА ЮРИДИЧЕСКИ ЛИЦА),

Личните данни се събират при сключване на договор с посочените лица (физически/юридически), като обичайно личните данни се съдържат в текста на самите договори.

РЕГИСТЪР „ВИДЕОНАБЛЮДЕНИЕ“ –КАМЕРИ, осъществява се с единствена цел- осигуряване безопасността- срок за съхранение -30дни

РЕГИСТЪР „ГОСТИ ХОТЕЛ“ ЗА ТОБО ХОТЕЛИ ООД-ХОТЕЛ „ЛАТИНКА“ И ХОТЕЛ „ВЕЛЕКА“

Регистри по изискванията на Закона за туризма, Закона за гражданската регистрация, Закон за чужденците в Република България – ТУРИСТИЧЕСКИ РЕГИСТРИ

ТОБО – ХОТЕЛИ ООД, съгласно договор за съвместна дейност с фирма ТОБО ООД, е обработващ лични данни на лицата, отседнали в хотелите Латинка – София, ул. Латинка 28А, и Велека – Черноморец, ул. Велека 9.

Създават се регистри по образци съгласно изискванията на Закона за туризма, Закона за гражданската регистрация, Закон за чужденците в Република България.

По същност и правно-нормативна основа адресната регистрация в хотелите е задължителна съгласно Закона за гражданската регистрация и Закона за пребиваване на чужденци в България. Това е дейност, свързана с гарантиране на сигурността и обществения ред в страната и в съответното заведение за пребиваване. Спрямо чужденците това е форма за установяване на временното им пребиваване в страната и визовите подробности. Всички пребиваващи в заведенията за пребиваване подлежат на адресна регистрация. Тя се извършва с предоставени документи за самоличност и служат за попълване на следните регистри по образец:

- Регистър за настанени туристи, по образец по чл. 116 (2) от Закона за туризма.
- Необходими данни: Име на лицето (за български граждани - на кирилица, за чужденци - на латиница, съгласно националния документ), ЕГН / ЛНЧ, Дата на раждане, Пол, Гражданство, Номер на лична карта/ Валиден национален документ за самоличност, Държава, издала националния документ, Дата на пристигане, Дата на отпътуване, Етаж, Стая, Апартамент, брой реализирани нощувки.

- За нуждите на МВР:

– Ежедневен рапорт за настанените лица с български паспорт и адресни карти по образец. Необходими данни: Име, пол, ЕГН, Номер на паспорт, Дата на издаване, Дата на валидност, Дата на раждане, номер на стая, брой нощувки.

-Ежедневен рапорт за чуждестранни граждани, изпращан онлайн в специален утвърден от МВР текстови файл.

Необходими данни: име, националност, номер на паспорт, дата на раждане, пол, дата на настаняване, стая.

- За извършване на основната икономическа дейност на дружеството – хотелско настаняване: Регистър Резервации:

Обработваните данни са: Име, телефон за връзка, електронна поща за контакт, дата на настаняване, дата на напускане, стая;

- За извършване на плащане на ПОС терминал по искане на госта: име, фамилия, вид на банкова карта;

(3) Данните се съхраняват на едно работно място в защитени с парола файлове и се обработват от лица, заемащи длъжности – Главен администратор, Администратор и Рецепционист.

За хотел Велека, град Черноморец, лицето, обработващо личните данни, е с длъжност: „Домакин“.

(4) Достъпът на външни лица до данните е забранен.

РЕГИСТЪР „ВИДЕОНАБЛЮДЕНИЕ“ ЗА ТОБО ХОТЕЛИ ООД - КАМЕРИ,

осъществява се с единствена цел- осигуряване безопасността

Регистър „Видеонаблюдение“ се попълва с данни от автоматично денонощно видеонаблюдение (видео образ) за движението на служителите и посетителите към подходите на сградите на ДРУЖЕСТВОТО и помещенията с определен статут. Записите с видео образи се съхраняват на отделен персонален компютър. За работа със записите от видеонаблюдението е обучен главният администратор, който прави това единствено и само по искане на управителя на дружеството и на легитимирани контролни държавни органи за установяване на извършени нарушения и престъпления.

(2) Данните в регистъра се предоставят доброволно от лицата при влизането им в сградата на ДРУЖЕСТВОТО. На входовете на сградата са поставени предупредителни табели, че обектът се намира под постоянно видеонаблюдение. Данните от този регистър се съхраняват 72 часа и служат за осигуряване на сигурността на обекта и предотвратяване на нарушения на обществения ред.

(3) Наблюдават се 4 сектора от територията на Дружеството – Вход, Паркинг, подход към Закрит гараж, Фоайе.

Чл. 14. Форми на водене на регистрите

По регистър „ФИНАНСОВО –СЧЕТОВОДЕН“ И РЕГИСТЪР „ЧОВЕШКИ РЕСУРСИ“

(1) На хартиен носител:

1. Форма на организация и съхраняване на личните данни - писмена (документална), съхраняват се в папки (кадрови досиета) за всеки служител или наето по граждански договор лице, както и за всеки клиент. Кадровите досиета се подреждат в специален картотечен шкаф със заключване;

2. Местонахождение на картотечния шкаф - поставен в помещение, предназначено за самостоятелна работа на обработващия/оператора на лични данни -Счетоводен отдел- „Човешки ресурси“)

3. Носител (форма) за предоставяне на данните от физическите лица - личните данни за всяко лице от посочения по-горе кръг от лица се набират в изпълнение на нормативно задължение - разпоредбите на Кодекса на труда и подзаконовите нормативни актове за прилагането му, Кодекса за социално осигуряване, Закона за счетоводството и други чрез:

-устно интервю с лицето (при постъпване или в процеса на работа, съответно при преговори с клиента),

-хартиен носител - писмени документи - молби, заявления за постъпване/извършване на работа по трудово или гражданско правоотношение, договорни отношения с клиенти, за изменение или прекратяване на тези отношения, по текущи въпроси в процеса на работа,

подадени от лицето, както и от външни източници (от съдебни, финансови, осигурителни, данъчни и други институции в изпълнение на нормативни изисквания). Личните данни от лицата се подават на администратора на лични данни и оправомощеното лице, назначено за обработването им - **обработващ/оператор на лични данни**, на основание нормативно задължение във всички случаи, когато е необходимо;

4. Достъп до личните данни - такъв има само обработващият/операторът на лични данни. (В случая-работещите в Счетоводен отдел (Човешки ресурси).

Възможността за предоставяне другиму достъп до личните данни при обработката им е ограничена и изрично регламентирана по-долу в чл. 6 "Задължения на обработващия/оператора на лични данни";

(2) На технически носител:

1 Форма на организация и съхраняване на личните данни - личните данни се съхраняват на твърд диск, на изолиран компютър. Компютърът е свързан в локална мрежа, със защитен достъп до личните данни, който е непосредствен само от страна на оператора на лични данни. При работа с данните се използват лицензиран софтуерни продукти по обработка на данните относно възнагражденията на персонала и клиентите, в това число основни и допълнителни възнаграждения, данъчни и други (вноски по заеми, запори и пр.) задължения, трудов стаж, присъствени и неприсъствени дни и други подобни.(фирма ПЛЮС-минус). Софтуерните продукти са адаптирани към специфичните нужди на администратора на лични данни. ТОБО ООД ползва услугите на фирма „ПЛЮС-МИНУС“.

2. Местонахождение на компютъра - в изолирано помещение за самостоятелна работа на оператора на лични данни по регистъра, но когато не е налице организационно-техническа възможност за това, компютърът може да бъде поставен в общо помещение за работа на обработващия лични данни с изпълняващи други дейности-вслучая-Счетоводен отдел,винаги заключен, достъп-ограничен.

3. Достъп до личните данни и защита - достъп до операционната система, съдържаща файлове за обработка на лични данни, има само обработващият/операторът на лични данни чрез парола за отваряне на тези файлове (свързаните с възнагражденията), известна на него, а в негово отсъствие - на временно упълномощено от него лице. Защитата на електронните данни от неправомерен достъп, повреждане, изгубване или унищожаване се осигурява посредством поддържане на антивирусни програми, периодично архивиране на данните на отделни дискове, както и чрез поддържане на информацията на хартиен носител.

Чл. 15. Групи данни в регистъра „Финансово –счетоводен“ и Регистър „Човешки ресурси“

(1) Относно **физическата идентичност** на лицата - имена и данни по лична карта (ЕГН, номер на лична карта, дата и място на издаване, адрес, месторождение, телефони за връзка и др.);

(2) Относно **семейна идентичност** на лицата (важи само за регистър "Служители") - семейно положение - брой членове на семейството, в това число деца до 18 години - данните са необходими при установяване правата на лицата за получаване на семейни добавки за деца до 18 години, за начисляване на съответни удържки от трудовото възнаграждение на дадено лице на основание присъдена издръжка, като критерий при подбор на служителите и други подобни;

(3) **Образование** (важи само за регистър "Служители")

- вид на образованието, място, номер и дата на издаване на дипломата - данните са необходими с оглед спазване нормативни или установени със щатното разписание на длъжностите изисквания за заемане, респ. за освобождаване на длъжности от лицата.

Предоставят се от лицата на основание нормативно задължение във всички случаи, когато е необходимо;

- **допълнителна квалификация** - данните са необходими с оглед спазване на нормативни или установени със щатното разписание на длъжностите изисквания за заемане, респ. за освобождаване на длъжности от лицата. Предоставят се от лицата на основание нормативно задължение във всички случаи, когато е необходимо;

(4) **Трудова дейност** (важи само за регистър "Служители") - професионална биография - данните са от значение при избора на подходящо за съответната длъжност лице. Предоставят се на основание нормативно задължение във всички случаи, когато е необходимо;

(5) Други - лични данни относно гражданско-правния статус на лицата, необходими за длъжностите, свързани с материална отговорност, като **свидетелство за съдимост**. Предоставят се на основание нормативно задължение.

Чл. 16. Задължения на лицето, отговарящо за водене и съхраняване на данните в регистъра

Задълженията на лицето, отговарящо за водене и съхраняване на данните в регистъра (оправомощеното лице) включват набиране, обработване, актуализация и съхраняване на лични данни, както следва:

1. Личните данни в **регистър "Служители"** се набират при постъпване/възлагане на работа по трудово или гражданско правоотношение на дадено лице чрез устно интервю и/или на хартиен носител, при което служителят **подписва изрично Съгласие за предоставянето на личните си данни за обработка на фирма ТОВО**.

2. Личните данни в **регистър "Клиенти"** се набират при воденето на преговори и съответно възлагане на поръчки от съответния клиент и подписване на договор.

Личните данни, събирани и обработвани от Администратора, се предоставят с цел изпълнението на договор, по който субектът на данните е страна, или за предприемане на стъпки по искане на субекта на данните, преди сключване на договор, свързан с **цялостната дейност на Администратора-ТОВО**, а именно:

- извършване на действия по проучване, проектиране и писмена кореспонденция с клиентите, относно техните недвижими имоти-парцели, апартаменти, сгради, офиси и други обекти;

- сключване на договор за търсене на подходящи недвижими имоти.

- сключване на договор за покупка /продажба/изграждане /наем на недвижими имоти;

- други.

За необходимостта от набиране на лични данни и конкретните цели, за които ще бъдат обработвани/използвани, обработващият личните данни информира лицето, което подписва изрично Съгласие за предоставянето на личните си данни за обработка на фирма ТОВО. (изготвен формуляр)

3. Обработване - обикновено личните данни се предоставят на представляващия администратора на лични данни чрез устно интервю и/или на хартиен носител. След одобрение на молбата за постъпване/възлагане на работа на лицето и/или съответно сключване на договор с клиент(като основен хартиен носител на лични данни), всички документи, съдържащи лични данни, заедно с приложенията към тях, се предават на обработващия/оператора на лични данни за оформяне на съответното правоотношение на технически и хартиен носител (изготвяне на трудов или граждански договор, или Договор за покупко –продажба на имот, или друго),

Изготвеният договор на технически носител остава в отделен файл на компютъра, като достъп до него има само обработващият/операторът на лични

данни.

Хартиеният носител се подрежда в кадрово досие на **клиента** или **постъпващото на работа** лице, заедно с останалите му документи с, съответно в картотечен шкаф със заключване, а препис от съответния договор - се връчва на клиента или постъпващия на работа;

4. Освен посочените лица и при посочените случаи, ограничен достъп до лични данни има освен главния счетоводител, и другите счетоводители, при обработване личните данни на лицата относно изготвяне на разплащателни документи, свързани с преводи на дължими суми на клиенти и/или възнагражденията на лицата, наети по трудови и граждански правоотношения в дружеството по банков път;

5. При необходимост от поправка на личните данни, лицата предоставят такива на обработващия/оператора на лични данни по негово искане на основание нормативно задължение.

6. Адресът, на който се приемат молби за достъп и предоставяне на лични данни от регистрите на ТОВО ООД, е както следва: гр. София ул. „Капитан Андреев”№5, или на електронен адрес: tobo-bg@tobo-bg.com.

Чл. 17. Актуализация на лични данни

(1) **Актуализация на лични данни** представлява допълнение или изменение на съществуваща информация в дружеството. Актуализация на лични данни се извършва:

- по искане на лицето, за което се отнасят личните данни, когато то е установило, че е налице грешка или непълнота в тях, и удостовери това с документ;
- по инициатива на обработващия лични данни - при наличие на документ, даващ основание за актуализация;
- при установена грешка при обработката на личните данни от страна на ТОВО
- ежемесечно-съгласно изискванията на Регламенат –GDPR.

(2) При актуализация на лични данни в досието на съответното лице се отразяват регистрационния номер на документа, източник на данните за актуализацията, дата на актуализацията. Актуализацията се извършва от лицето,определено за **«обработващ лични данни»**.

VII. МЕРКИ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

Чл.18. Мерки за защита при обработване на личните данни

(1) технически мерки

Правилата за защита при обработване на лични данни регламентират мерки, които:

- отхвърлят достъпа на неоторизирани лица до оборудването за обработка на данни – контрол на достъпа до оборудване;
- предотвратяват неоторизираното четене, копиране, промяна или унищожаване на информационни носители - контрол на информационните носители;
- предотвратяват неоторизираното добавяне, въвеждане, преглеждане, промяна или заличаване на съхранени лични данни - контрол по съхраняването;
- предотвратяват използването му от неоторизирани лица, използващи комуникационно оборудване за данни - контрол на потребителите;
- гарантират, че лицата, които са оторизирани да ползват система за автоматизирана обработка на данни, имат достъп **само до данните, включени в обхвата на техния достъп** - контрол на достъпа до данни;
- осигуряват възможността за проверка и установяване до кои органи са били или могат да бъдат изпратени или предоставени личните данни чрез използване на комуникационно оборудване за данни - контрол на комуникациите;
- осигуряват възможност за последваща проверка и установяване какви лични данни са въведени в системите за автоматизирана обработка на данни, кога и от кого са въведени данните - контрол на въвеждане;

- предотвратяват неототоризирано четене, копиране, промяна или изтриване на лични данни при трансфер на лични данни или превозване на носители на данни - контрол при транспортиране;
- осигуряване на възможност инсталираните системи да могат да се възстановят в случаи на прекъсване на функционирането - възстановяване;
- осигуряват правилното функциониране на системата, докладване на появата на грешки във функциите (надеждност) и гарантират, че съхранените данни не могат да бъдат повредени чрез неправилно функциониране на системата - интегритет.
- Служителите, обработващи лични данни, вземат мерки за гарантиране на надеждност при обработването, като осъществяват технически и организационни мерки за защита на личните данни.

(2) При автоматичната обработка на лични данни се осъществяват технически мерки за защита срещу:

- неототоризирано четене, възпроизвеждане, промяна или премахване на носителя на данните;
- неототоризирано въвеждане, промяна или заличаване на съхранени лични данни;
- неототоризирано използване на системите за лични данни чрез средства за пренос на данни;
- неототоризиран достъп до лични данни.

(2) Мерки за документална защита

- Дружеството установява процедури по обработване на лични данни, регламентиране на достъпа до данните, процедури по унищожаване и срокове за съхранение, подробно разписани в тези Правила. За отделни категории данни може да се предвиди псевдонимизиране по предложение на Лицето, отговорно за личните данни.
- Размножаването и разпространението на документи или файлове, съдържащи лични данни, се извършва само и единствено от упълномощени служители при възникнала необходимост.
- **Периодично архивиране и актуализиране**

Архивиране на личните данни на технически носител се извършва **периодично на всеки един месец** от обработващия/оператора на лични данни с оглед запазване на информацията за съответните лица в актуален вид. Същото се извършва на дискове, достъп до които има само обработващият/операторът на лични данни.

(3) Персонални мерки на защита

- Преди заемане на съответната длъжност лицата, които осъществяват защита и обработване на личните данни:
 - поемат задължение за неразпространение на личните данни, до които имат достъп;
 - се запознават с нормативната база, вътрешните правила и политики на дружеството 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 тези Правила ред.
- При постъпване на работа всички служители 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 персонала се провеждат периодично, за да се гарантира познаване на нормативната уредба, потенциалните рискове за сигурността на данните и мерките за намаляването им.

(4) Мерки за защита на автоматизирани информационни системи и криптографска защита

- 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.
- Електронните бази данни са защитени посредством логически средства за защита, като антивирусна програма, която се обновява автоматично, защитни пароли и др.
- Архивиране на личните данни на технически носител се извършва периодично с оглед съхранение на информацията.
- Защитата на електронните данни от неправомерен достъп, повреждане, изгубване или унищожаване, извършени умишлено от лице или в случай на технически неизправности, аварии, произшествия, бедствия и 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).
- (2) Лицето, отговорно за личните данни, докладва периодично на ръководството на дружеството предприетите мерки за гарантиране нивото на сигурност при обработване на лични данни.

VIII. НАРУШЕНИЯ НА СИГУРНОСТТА

Чл. 19. (1) Лицата, идентифицирали признаци на нарушение на сигурността на данните, са длъжни да докладват незабавно на Лицето, отговорно за личните данни, като му предоставят цялата налична информация.

(2) Лицето, отговорно за личните данни, извършва незабавно проверка по подадения сигнал, като се опитва да установи дали е осъществено нарушение на сигурността и кои данни са засегнати.

(3) Лицето, отговорно за личните данни, докладва незабавно на съдружниците в Дружеството наличната информация за нарушението на сигурността, включително информация относно характера на инцидента, времето на установяването му, вида на щетите, предприетите към момента мерки и мерките, които счита, че трябва да се предприемат.

(4) След съгласуване с ръководството на дружеството, Лицето, отговорно за личните данни, предприема мерки за предотвратяване или намаляване последиците от пробива и възможностите за възстановяване на данните.

(5) При спешност, когато съгласуване с ръководството би забавило реакцията и би нанесло големи щети, Лицето, отговорно за личните данни, може по своя преценка да предприеме мерки за предотвратяване или намаляване последиците от нарушението на сигурността. В този случай Лицето, отговорно за личните данни, уведомява незабавно ръководството за предприетите мерки и съобразява последващи действия с получените инструкции.

Чл. 20. (1) В случай че нарушението на сигурността създава вероятност от риск за правата и свободите на физическите лица, чиито данни са засегнати, и след одобрение от ръководството на дружеството, Лицето, отговорно за личните данни, организира уведомяването на КЗЛД.

(2) Уведомяването на КЗЛД следва да се извърши без ненужно забавяне и когато това е осъществимо – не по-късно от 72 часа след първоначалното узнаване на нарушението.

(3) Уведомлението до КЗЛД съдържа следната информация:

(а) описание на нарушението на сигурността; категориите и приблизителният брой на засегнатите субекти на данни и категориите и приблизителното количество на засегнатите записи на лични данни;

(б) името и координатите за връзка на Лицето, отговорно за личните данни;

- (в) описание на евентуалните последици от нарушението на сигурността;
 - (г) описание на предприетите или предложените мерки за справяне с нарушението на сигурността, включително мерки за намаляване на евентуалните неблагоприятни последици.
- (4) Когато има вероятност нарушението на сигурността на личните данни да породи висок риск за правата и свободите на физическите лица, Лицето, отговорно за личните данни, без ненужно забавяне и при спазване на приложимото законодателство уведомява засегнатите физически лица.

Чл. 21. (1) Дружеството води регистър на нарушенията на сигурността, който съдържа следната информация:

- (а) дата на установяване на нарушението;
- (б) описание на нарушението – източник, вид и мащаб на засегнатите данни, причина за нарушението (ако е приложимо);
- (в) описание на извършените уведомявания: уведомяване на КЗЛД и засегнатите лица, ако е било извършено;
- (г) предприети мерки за предотвратяване и ограничаване на негативни последици за субектите на данни и за Дружеството;
- (д) предприети мерки за ограничаване на възможността от последващи нарушения на сигурността.

(2) Регистърът се води в електронен формат от Лицето, отговорно за личните данни.

IX. ПРЕДОСТАВЯНЕ НА ЛИЧНИ ДАННИ НА ТРЕТИ ЛИЦА

Чл.22. Предоставяне на лични данни на трети лица

(1) Дружеството може при необходимост да предоставя лични данни на трети лица, действащи в качеството на обработващ, въз основа на изричен договор. (пример-Договор със Служба за трудова медицина) съвместна дейност

(2) В случаите на предоставяне на данните на служители, клиенти или доставчици на услуги на обработващ, Дружеството:

- (а) изисква достатъчно гаранции от обработващия за спазване на законовите изисквания и добрите практики за обработка и защита на личните данни;
- (б) сключва писмено споразумение или друг правен акт с идентично действие, който урежда задълженията на обработващия и отговаря на изискванията на чл. 28 от Регламент (ЕС) 2016/679;

(в) информира физическите лица, чиито данни ще бъдат предоставени на обработващ.

(3) Правомерен достъп на трети лица до кадровите досиета на персонала и клиентите

(а) Кадровото досие на лицето не се изнася извън сградата на администратора. Никое оправомощено или трето лице няма право на достъп до кадровите досиета на персонала и клиентите на дружеството, освен ако същото е изисквано по надлежен път от органи на надзора или на съдебната власт (Комисия за финансов надзор, съд, прокуратура, следствени органи, Контролни органи-Инспекция по труда и др.). Достъпът на тези органи до личните данни на лицата е правомерен.

(б) Надлежен е начинът, при който съответният орган е изискал кадрово досие или данни, съдържащи се в него, писмено с изрично искане, отправено до Управителите на дружеството. В подобни случаи на заявителя се предоставя копие от съдържащите се в кадровото досие документи, заверени с подпис на оператора на лични данни и печат на дружеството. За идентичността на предоставените копия от документи с оригиналите им отговорност носи операторът. В подобни случаи и ако в писменото искане на съответния орган не се съдържа изрична забрана за разгласяване, операторът на лични данни е длъжен да информира лицето, но не и да пречатства работата на надлежните органи.

(в) Не се изисква съгласие на лицето, ако обработването на неговите лични данни се извършва само от или под контрола на компетентен държавен орган за лични данни,

свързани с извършване на престъпления, на административни нарушения и на непозволені увреждания. На такива лица се осигурява достъп до личните данни, като при необходимост им се осигуряват съответни условия за работа в помещение на дружеството.

(г) Правомерен е и достъпът на ревизиращите държавни органи, надлежно легитимирани се със съответни документи - писмени разпореждания на съответния орган, в които се посочва основанието, имената на лицата, като за целите на дейността им е необходимо да им се осигури достъп до кадровите досиета на персонала или клиентите.

(д) При промени в статута на дружеството (преобразуване, ликвидация и други), налагащи прехвърляне на регистрите за лични данни от дружеството на друг администратор на лични данни, предаването на регистъра се извършва след разрешение на Комисията за защита на лични данни.

(е) Решението си за предоставяне или отказване достъп до лични данни за съответното лице администраторът(ТОБО) съобщава на третите лица в 30-дневен срок от подаване на молбата, респ. искането.

(ж) При внедряване на нов програмен продукт за обработване на лични данни се извършва предварителна проверка на възможностите на продукта с оглед спазване изискванията на ЗЗЛД и Регламента, и осигуряване максималната им защита от неправомерен достъп, загубване, повреждане или унищожаване.

(з) За неизпълнение на задълженията, вменени на съответните оправомощени лица по тази инструкция и по ЗЗЛД и Регламента, се налагат дисциплинарни наказания по Кодекса на труда, а когато неизпълнението на съответното задължение е констатирано и установено от надлежен орган - предвиденото в ЗЗЛД административно наказание - глоба.

(3) Обработване на лични данни от обработващи извън ЕС/ЕИП е допустимо само когато:

(а) Европейската Комисия е приела решение, потвърждаващо, че страната, към която се извършва трансферът, осигурява адекватно ниво на защита на правата и свободите на субектите на данни;

(б) Налице са подходящи мерки за защита – като например Обвързващи Корпоративни Правила (ОКП), стандартни договорни клаузи, одобрени от Европейската Комисия, одобрен кодекс за поведение или сертификационен механизъм;

(в) Субектът на данни е дал своето изрично съгласие за трансфера, след като е информиран за възможните рискове, или

(г) Трансферът е необходим за една от целите, изброени в ОРЗД, включително изпълнението на договор със субекта, защита на обществения интерес, установяване и защита на правни спорове, защита на жизненоважните интереси на субекта на данни в случаите, когато той е физически или юридически неспособен да даде съгласие.

Х. ОЦЕНКА НА ВЪЗДЕЙСТВИЕТО ВЪРХУ ЗАЩИТАТА НА ДАНИТЕ

Чл. 23. (1) Оценка на въздействието се извършва, когато това се изисква съгласно приложимото законодателство и с оглед на риска за физическите лица и естеството на обработка на лични данни, извършвана от Дружеството. Оценка на въздействието се извършва за високорискови дейности по обработване.

(2) Оценка на въздействието е необходимо при всяко въвеждане на ключова система или смяна на бизнес програма, която е свързана с обработване на лични данни, включително:

- първоначалното въвеждане на нови технологии или прехода към нови технологии;
- автоматизирано обработване, включително профилиране или автоматизирано вземане на решения;
- обработване на чувствителни лични данни в голям мащаб;
- мащабно, систематично наблюдение на публично обществена зона.

(3) За оценката се съставя протокол, който се предоставя при поискване от страна на КЗЛД.

XI. УНИЩОЖАВАНЕ НА ДАННИТЕ

Чл. 24. (1) Унищожаване на личните данни се извършва от Дружеството или изрично упълномощено лице, без да бъдат накърнявани правата на лицата, за които се отнасят данните, обект на унищожаването, и при спазване на разпоредбите на относимите нормативни актове.

(2) Информацията в регистрите се унищожават след постигане на целите на обработката и при отпаднала необходимост за съхранение.

(3) Унищожаването на данни на хартиен носител се извършва чрез нарязване с шредер машина. Електронните данни се изтриват от електронната база данни по начин, непозволяващ възстановяване на информацията.

XII. ЛИЦА, ОТГОВАРЯЩИ ЗА СЪБИРАНЕТО, ОБРАБОТКАТА И СЪХРАНЕНИЕТО НА ЛИЧНИТЕ ДАННИ И ДОСТЪП ДО ЛИЧНИ ДАННИ ПРАВОМЕРЕН ДОСТЪП ДО ЛИЧНИ ДАННИ

Чл. 25. Лицето, отговорно за личните данни, и лицата, обработващи личните данни от името на дружеството, са физически или юридически лица, притежаващи необходимата компетентност и назначени и/или упълномощени със съответен писмен акт, включително и чрез настоящите Правила.

Чл. 26. (1) Лицето, отговорно за личните данни:

- подпомага Дружеството и лицата, обработващи личните данни при изпълняване на задълженията им по защита на личните данни, като осигурява прилагането и поддържа необходимите технически и организационни мерки и средства за осъществяване на защитата на данните;
- осигурява нормалното функциониране на гореспоменатите системи за защита;
- осъществява контрол през целия процес на събиране и обработване на данните;
- изпълнява всички задължения по докладване и управление на нарушения на сигурността на данните;
- периодично изисква информация от лицата, обработващи лични данни, във връзка със събирането, достъпа и обработването им;
- уведомява Дружеството своевременно за всички нередности, установени във връзка с изпълнение на задълженията му;
- унищожават данните от хартиените и техническите носители съгласно закона и сроковете, установени в тези Правила;
- преупълномощава физически или юридически лица с писмен акт, които да осъществяват защитата на личните данни.

(2) **Контрол при обработване на личните данни**

Контролът върху дейностите по обработка на лични данни ТОВО се осъществява от заемащ длъжността «Длъжностно лице по защита на данните»

Чл. 27. (1) Събирането, обработката, съхранението и защитата на личните данни се извършва само от лица, на които това е изрично указано и чиито служебни задължения или конкретно възложена задача налагат това.

(2) При възлагане на дейности, налагащи обработката на лични данни от регистрите на дружеството, доставчиците на услуги следва да спазват приложимите нормативни изисквания относно обработката на личните данни и процедурите на чл. 19 от тези Правила.

(3) Достъп до личните данни могат да имат и съответните държавни органи – съд, следствие, прокуратура, ревизиращи органи и др. Гореспоменатите могат да изискат

данните по надлежен ред във връзка с изпълнението на техните правомощия.

XIII. ПРАВА НА СУБЕКТИТЕ НА ДАННИ

Чл. 28. Права на субектите на данни- Осигуряване на достъп на лицата до личните им данни

(1) Достъп до личните данни на лицата, съдържащи се на технически носител има само обработващият/операторът на лични данни, а в негово отсъствие и когато тези данни се отнасят до възнагражденията на лицата, достъп до тях има временно упълномощено от обработващият/операторът на лични данни лице, комуто е известна паролата за достъп до файловете.

(2) Всяко лице има право да иска достъп до своите лични данни, включително и да иска потвърждение дали данните, отнасящи се до него, се обработват, да се информира за целите на това обработване, категориите данни и за получателите на данните, както и за целите на всяко обработване на лични данни, отнасящи се до него.

(3) Правото на достъп се осъществява чрез искане на засегнатото физическо лице, подадено писмено в заявление до обработващия/оператора на лични данни, в това число и по електронен път, лично или чрез упълномощено лице. и получено на адреса по седалището на Дружеството .

Заявлението съдържа име на лицето и други данни, които го идентифицират - длъжност, месторабота, описание на искането, предпочитана форма за предоставяне достъпа до лични данни, подпис, дата и адрес на кореспонденцията; пълномощно - когато заявлението се подава от упълномощено лице.

Достъп до данните на лицето се осигурява под формата на:

1. устна справка;
2. писмена справка;
3. преглед на данните от самото лице или упълномощено от него такова;
4. предоставяне на копие от исканата информация.

Когато данните не съществуват или не могат да бъдат предоставени на определено правно основание, на заявителя се отказва достъп до тях с мотивирано решение. Отказът за предоставяне на достъп може се обжалва от лицето пред посочения в писмото орган и срок

(4) Всяко физическо лице има право да поиска заличаването, коригирането или блокирането на негови лични данни, обработването на които не отговаря на изискванията на закона.

(5) Всяко лице има право писмено да възрази срещу обработването на и/или предоставянето на трети лица на неговите лични данни без необходимото законово основание.

(6) Дружеството е длъжно в двуседмичен срок от получаване на искане по предходните алинеи да уведоми заявителя дали са налице законовите основания за уважаване на искането. Ако Дружеството установи, че са налице законовите основания да уважи искането, уведомява лицето и за реда, по който може да упражни правото си.

(7) Субектите на данни имат също правото да:

- оттеглят съгласието си за обработване по всяко време;
- възразят срещу употреба на личните им данни за целите на директния маркетинг;
- изискат информация за основанието, въз основа на което личните им данни са предоставени за обработване на обработващ извън ЕС/ЕИП;
- възразят срещу решение, взето изцяло на база на автоматизирано обработване, включително профилиране;
- бъдат уведомени за нарушение на защита на данните, което е вероятно да доведе до висок риск за техните права и свободи;
- подават жалби до регулаторния орган;
- в някои случаи да получат или да поискат техните лични данни да бъдат трансферирани до трета страна в структуриран, общо използван формат, подходящ за машинно четене (право на преносимост).

XIV. ДЕФИНИЦИИ

Чл. 29 За целите на настоящите Правила, използваните понятия имат следното значение:

- **ЗЗД** – Закон за защита на личните данни.
- **КЗЛД** – Комисия за защита на личните данни.
- **ОРЗД** – Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 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 (Общ регламент относно защитата на данните).
- **Длъжностно лице** по защита на данните – физическо лице или организация, определени съгласно изискванията на чл. 37 ,ОРЗД, или – Лице, отговорно за личните данни –
- **Администратор на лични данни** – ТОБО ООД, който определя целите и средствата за обработването на лични данни. „Администратор“ обозначава ТОБО /Дружеството.
- **Обработващ лични данни** – лице или организация, което въз основа на договор обработва лични данни, предоставени от Дружеството, за уговорените цели.
- **Известия** по защита на данните – отделни известия, съдържащи информация, предоставяна на субектите на данни в момента, в който Дружеството събира информация за тях. Тези известия могат да бъдат както общи (напр. адресирани към работници и служители или известия на уебсайта на организацията), така и отнасящи се до обработване със специфична цел.
- **Обработване на данни** – всяка дейност, която е свързана с използването на лични данни. Това включва: получаване, записване, съхранение, извършване на операция или серия от операции с данните като напр. организиране, редактиране, възстановяване, използване, предоставяне, изтриване или унищожаване. Обработването също включва и трансфер на лични данни до трети лица.
- **Псевдонимизиране** – заместването на информация, която директно или индиректно идентифицира физическо лице, с един или повече идентификатори („псевдоними“), така че лицето да не може да бъде идентифицирано без достъп до допълнителната информация, която следва да се съхранява отделно и да е поверителна.
- **Съгласие** – всяко свободно изразено, конкретно, информирано и недвусмислено указание за волята на субекта на данни, посредством изявление или ясно потвърждаващо действие, което изразява съгласие за обработка на лични данни, свързани с него.

XV. Допълнителни разпоредби “.

Чл.30. Дружеството може да променя тези Правила по всяко време.

Всички промени следва да бъдат незабавно сведени до знанието на лицата, които засягат. Настоящите Правила подлежат на утвърждаване от Управителя на ТОБО ООД, гр. София и всички служители на дружеството следва да бъдат запознати с нея.

Настоящите Правила са приети и влизат в сила в деня на подписването им.

УТВЪРЖДАВАМ: _____

ИНЖ. АНТОН МАЖДРАКОВ

25.април 2018г

УПРАВИТЕЛ