Общи условия за обработка на данни в съответствие с член 28 от Общия регламент за защита на личните данни (ОРЗЛД)

1. Предмет и срок

(1) Настоящите Общи условия уреждат условията, при които А1 България ЕАД, с адрес на управление гр. София, ул. „Кукуш" №1, ЕИК 131468980 (наричано по-нататък „Обработващият") извършва обработка на данни въз основа на договор за услуги (наричан по-нататък „Договорът за услуги"), сключен между него и лице, което е администратор на съответните данни по смисъла на ОРЗЛД (наричано по-нататък „Администраторът").

(2) Естеството, обемът и целта на планираната обработка на лични данни от Обработващия за Администратора се определят от Договора за услуги

(3) Срокът на обработка на данни съгласно настоящите Общи условия съответства на срока на Договора за услуги.

(4) Само ако в Договора за услуги е предвидено прехвърляне на лични данни в трета страна (която не е Страна член нито на ЕС, нито на ЕИП) обработката ще се извършва, само ако специалните изисквания на член 44 и следващите от ОРЗД са изпълнени. и адекватното ниво на защита в тази трета страна:

А) е определено от Европейската комисия (член 45, параграф 3 от ОРЗД); или

Б) е резултат от задължителни фирмени правила (член 46, параграф 2, буква б във връзка с член 47 от ОРЗД); или

В) е резултат на Стандартни клаузи за защита на данни (член 46, параграф 2, точки в и г от ОРЗД); или

Г) е резултат на одобрен Кодекс за поведение (член 46, параграф 2, буква д във връзка с член 40 от ОРЗД); или

Д) е резултат на одобрен Механизъм за сертифициране (член 46, параграф 2, буква е във връзка с член 42 ОРЗД); или

Е) е установено по друг начин (член 46, параграф 2, буква а, параграф 3, точки а и б от ОРЗД).

2. Технически и организационни мерки

(1) Преди началото на обработката, Обработващият ще документира нужните Технически и организационни мерки.

(2) Обработващият ще осигури сигурността в съответствие с член 28, параграф 3, буква в, във връзка с член 5, параграф 1 и параграф 2 от ОРЗД. Мерките гарантират ниво на сигурност, адекватно на риска, касаещ поверителност, интегритет, наличност и устойчивост на системите. Освен ако друго не е предвидено в Договора за услуги, Обработващият ще носи отговорност за осигуряване на нивото на сигурност, адекватно за съответната обработка.

3. Коригиране, ограничаване и изтриване на данни

(1) Само в съответствие с документираните указания на Администратора, Обработващият може да коригира, изтрива или ограничава обработката на данни. В случай че Субект на данни се

свърже директно с Обработващия относно коригиране, изтриване или ограничаване на обработката, Обработващият незабавно ще препрати искането на Субектите на данни към Администратора.
(2) Доколкото е включено в обхвата на услугите за политиката по изтриване, „правото да бъде забравен“, коригирането, преносът на данни и достъпът, Обработващия ще съдейства на Администратора, в съответствие с документираните указания на последния.

4. Осигуряване на качество и други задължения на Обработващия

(1) В допълнение към спазване на правилата, установени в Общите условия и/или Договора за услуги, Обработващият ще спазва нормативните изисквания, посочени в членове от 28 до 33 от ОРЗД; съответно, Обработващият осигурява спазването на следните изисквания:

А) Писмено назначаване на Длъжностно лице по защита на данните, който изпълнява задълженията си по членове 38 и 39 от ОРЗД. Администраторът ще бъде информиран за съответните данни за осъществяване на връзка. Администраторът следва да бъде своевременно уведомен за каквато и да е промяна на Длъжностното лице по защита на данните.

Б) Поверителност в съответствие с член 28, параграф 3, буква б, членове 29 и 32, параграф 4 от ОРЗД. Обработващият ще поверява обработката на данни само на такива служители, които са обвързани от задължение за поверителност и преди това са запознати с разпоредбите за защита на данни, които се отнасят до работата им. Обработващият и което и да е друго лице, което действа под негово ръководство няма да обработват данни, освен ако нямат указания на Администратора за това.

В) Прилагането на и спазването на всички Технически и организационни мерки да бъде в съответствие с член 28, параграф 3, изречение 2, буква в и член 32 ОРЗД (съобразно описаното в Приложение № 1).

Г) Администраторът и Обработващият ще сътрудничат при поискване на надзорния орган при изпълнение на задачите му.

Д) Администраторът следва да бъде незабавно уведомен за каквито и да е проверки и мерки, предприети от надзорния орган, доколкото се отнасят до Договора за услуги. Това се отнася и за случаите, в които Обработващият е проверяван или е страна по проверка от компетентен орган във връзка с нарушение на който и да е нормативен акт, касаещ обработката на лични данни във връзка с изпълнението на настоящите Общи условия и/или Договора за услуги.

Е) В случай, че Администраторът е предмет на проверка от надзорния орган, при претенция за отговорност от страна на Субект на данни или от трета страна или на каквато и да е друга претенция във връзка с договор за обработка на данни, по който е страна Обработващият, Обработващият ще положи всички усилия, за да подпомогне Администратора.

Ж) Обработващият периодично ще преглежда вътрешните си процеси и Техническите и организационни мерки, за да осигури, че обработката в рамките на областта му на отговорност е в съответствие с изискванията на приложимия закон за обработка на данни и опазване на правата на Субекта на данни.

З) Възможност за потвърждаване на Техническите и организационни мерки, от страна на Администратора като част от надзорните правомощия на Администратора, упоменати в точка 6 от тези Общи условия.

5. Подизпълнители

(1) Възлагането на подизпълнители за целите на тези Общи условия ще се отнася до услуги, свързани пряко с предоставянето на основната услуга. Това не включва подпомагащи услуги, като електронни съобщителни услуги, пощенски/транспортни услуги, поддръжка и услуги по подпомагане на потребители или унищожаване на носители на данни, както и други мерки, които осигуряват поверителността, наличността, интегритета и устойчивостта на хардуера и софтуера за оборудването по обработка на данни. Обработващия, обаче е длъжен да осигури адекватни и правно обвързващи договорни връзки, за да гарантира защитата на данните и сигурността на данните на Администратора, дори и в случай на подпомагащи услуги, възложени на подизпълнители.

(2) Освен ако не е уговорено друго в Договора за услуги, Обработващият може да наеме допълнителни подизпълнители (оправомощени лица), които да подпомогнат обработката на данни по тези Общи условия. В този случай обработващият следва да изготви списък на всички подизпълнители и ако това бъде поискано, да изпрати копие от него на Администратора. В случай че има основателна причина, Администраторът може да откаже наемането на подизпълнител.

(3) Всички подизпълнители ще бъдат обвързани от същите задължения, както Обработващия по тези Общи условия или договорите, свързани с него.

(4) Обработващият по всяко време ще носи отговорност към Администратора за спазване на тези Общи условия и свързаните с него договори от страна на подизпълнителите.

6. Надзорни права на Администратора

(1) Администраторът има право, след консултации с Обработващия, да извърши проверки или да възложи извършването им от одитор за спазване на техническите и организационни мерки за сигурност, само ако:

А) Обработващият не е представил достатъчно доказателства за спазването на техническите и организационни мерки. В този случай Администраторът може да поиска Доклади на SOC Audit или представяне на сертификати по ISO/IEC 27001;

Б) Възникнало е нарушение на сигурността;

В) Администраторът има право на одит, съгласно действащото законодателство. (2) Администраторът следва да изпрати подробен план за одит/контрол на Обработващия поне две седмици преди насрочената дата на одита, в който се посочват обхата, продължителността на одита и началната дата на одита. Обработващият ще прегледа плана за одит/контрол и ще предостави на Администратора всякакви съществени опасения и въпроси, като например искания за информация, които могат да повлияят на сигурността, поверителността или политиката по наемане на хора на Обработващия. Във всеки случай, Обработващият ще съдейства на Администратора за съгласуването на окончателен план за одит/контрол.

(3) Проверката ще се осъществи в нормално работно време в съответствие с политиките за работа на съответното работно място на Обработващия и няма ненужно да нарушава работния процес на Обработващия. Обработващият ще положи разумни усилия да предостави на одитора поисканата от него информация.

(4) Доказателства за прилагането на техническите и организационни мерки, за изпълнение на задълженията, произтичащи от тези Общи условия могат да бъдат предоставени чрез:

А)Спазване на одобрените Кодекси за поведение съгласно член 40 от ОРЗЛД.

Б)Сертифициране в съответствие с одобрената процедура за сертифициране в съответствие с член 42 от ОРЗЛД;

В)Сертификати на одитора, доклади или извлечения от доклади предоставени от независими органи (напр. одитор, Длъжностно лице по защита на данните, Отдел по IT сигурност, одитор за поверителност на данни, одитор по качеството).

Г)Съответно сертифициране от одитиране по It сигурност или защита на данни (напр. ISO 27001/IEC).

Д)Годишни доклади от Обработващия.

(5) Всички разходи по извършване на одит/контрол са за сметка на Администратора.

7. Други задължения

(1) Обработващият ще подпомага Администратора при спазване на задълженията, касаещи сигурността на личните данни, изисквания за отчет при пробив на данни, оценки на въздействието на защитата на данни и предварителни консултации, упоменати в членове 32 до 36 от ОРЗД. Това включва:

А) Осигуряване на адекватно ниво на защита посредством Технически и организационни мерки, които вземат предвид обстоятелствата и целите на обработката, както и прогнозираната вероятност и тежест на възможно нарушение на закона в резултат на уязвимост на сигурността и които дават възможност за незабавно установяване на съответни случаи на нарушаване.

Б) Задължението за незабавно съобщаване на Администратора на пробив на лични данни.

В) Задължението за подпомагане на Администратора по отношение на задължението на Администратора за предоставяне на информация на засегнатия Субект на данни и незабавното предоставяне на Администратора на цялата относима информация в това отношение.

Г) подпомагане на Администратора при оценката му на въздействие върху опазването на данни.

Д) Подпомагане на Администратора по отношение на предварителните консултации с надзорния орган.

(2) Обработващият има право на възнаграждение за подпомагащите услуги, които не са включени в описанието на услугите и които не се дължат на неизпълнение от страна на Обработващия.

8. Правомощия на Администратора за даване на указания

(1) Администраторът незабавно ще потвърждава устните си указания с писмено изявление.

(2) Обработващият ще уведомява Администратора незабавно, ако смята, че дадено указание нарушава разпоредбите за защита на данни. В такъв случай Обработващият ще има право да преустанови изпълнението на съответните указания, докато Администраторът не ги потвърди или промени.

9. Изтриване и връщане на лични данни

(1) Копия или дубликати на данни няма да бъдат създавани без знанието на Администратора, с изключение на резервни копия, доколкото са нужни, за гарантиране на правилната обработка на данни, както и данните, нужни за изпълнение на регулаторни изисквания по отношение на съхранение и обработка на данни.

(2) След приключване на договорената работа или по-рано, по искане на Администратора, най-късно до прекратяване на Договора за услуги, Обработващият ще предаде на Администратора

или – при наличие на предварително съгласие – ще унищожи всички документи, резултати от обработване или използване и всички набори от данни, свързани с договора, които са в негово притежание при спазване на изискванията за опазване на данни.
(3) Документация, която се използва за демонстриране на правилната обработка на данни в съответствие с Договора за услуги и/или тези Общи условия ще бъде съхранявана от Обработващия и след момента в ал. 2 на този член, в срок, съобразно изискванията на действащото законодателство.

11. Приложим закон
(1) Настоящите Общи условия се подчинява изключително на българското право.
(2) Настоящите Общи условия се приемат от Администратора и Обработващия с подписването на съответния Договор за услуги.

Приложение №3.1 –Технически и организационни мерки

1. Поверителност (член 32, параграф 1, буква б от ОРЗД)

- Контрол на физическия достъп

Не се допуска непозволен достъп до Помещенията за обработка на данни, напр. магнитни или чип карти, ключове, електронни ключове за врата, охранителни услуги за помещения и/или охранителен персонал на входа, алармени ссистеми, видео/охранителни камери

- Електронен контрол на достъпа

Не се допуска непозволено използване на системите за обработка на данни или съхранение на данни, напр. (сигурни) пароли, механизми за автоматично блокиране/заключване, двустепенно разпознаване, шифроване на носители на данни/медия за съхранение

- Контрол на вътрешния достъп (разрешения за права на достъп на потребители до и изменение на данни)

Забранено е непозволеното Четене, Копиране, Промени или Изтриване на Данни вътре в системата, т.е. концепция за разрешаване на права, права за достъп само при нужда, регистриране на достъпа до системата

- Изолационен контрол

Изолираната Обработка на данни, която се събира за различни цели, напр. разнообразно съдействие на Контрольора, сандбоксинг;

- Псевдонимизация (член 32, параграф 1, буква а от ОРЗЛД; член 25, параграф 1 от ОРЗЛД)

Обработката на лични данни по такъв метод/начин, че данните да не могат да бъдат свързани с определен Субеект на данни без съдействието на допълнителна Информация, при условие че тази допълнителна информация се съхранява отделно и е предмет на адекватни технически и организационни мерки.

2. Интегритет (член 32, параграф 1, точка б от ОРЗЛД)

- Контрол на прехвърляне на данни

Забрана за непозволено Четене, Копиране, Промени или Изтриване на данни с електронен пренос или транспорт, т.е. криптиране, виртуални частни мрежи (Ви Пи Ен), електронен подпис;

- Контрол на постъпването на данни

Потвърждаване дали и от кого се въвеждат лични данни в Системата за обработка на лични данни, се променят или изтриват, напр. Влизане, Управление на документи

3. Достъпност и устойчивост (член 32, параграф 1, буква б от ОРЗЛД)

- Контрол на достъпността

Превенция на случайно или умишлено унищожаване или загуба, т.е. Стратегия за разервни копия (онлайн/офлайн, он-сайт/оф-сайт), Непрекъснат достъп на електричество (Ю Пи Ес), защита от вируси, файруол, процедури за отчет и планиране на случайни събития

- Бързо възстановяване (член 32, параграф 1, буква в от ОРЗЛД);

4. Процедури за редовни тестове, оценка и преценка (член 32, параграф 1, точка г от ОРЗД; член 25, параграф 1 от ОРЗЛД)

- Управление на защитата на данни
- Управление на докладването за инциденти
- Защита на данни чрез планиране и по подразбиране (член 25, параграф 2 от ОРЗЛД);
- Поръчка или договорен контрол

Забрана за обработка на данни от трети лица в съответствие с член 28 от ОРЗЛД без съответни указания от Контрольора, т.е. ясни и недвусмислени договорни ангажименти, формализирано управление на Поръчките, строг контрол при избора на Доставчик на услуги, задължение за предварителна оценка, последващи надзорни проверки.