Приложение № 5

СПОРАЗУМЕНИЕ ЗА ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ

МЕЖДУ АДМИНИСТРАТОР И ОБРАБОТВАЩ

съгласно Регламент (ЕС) 2016/679 на Европейския Парламент и на Съвета
от 27 април 2016 година

Днес……., в гр. София, между:

„ХОЛДИНГ БДЖ“ ЕАД, ЕИК 130822878 , със седалище и адрес на управление: гр. София, ул. „Иван Вазов“ № 3, представлявано от инж. Георги Друмев Друмев – Изпълнителен директор, наричано по-долу **(„Администратор”)** и

„……“, ЕИК ……., със седалище и адрес на управление: ……., представлявано от ……. – Управител, наричано за целите на това Споразумение по-долу **(„Обработващ”),**

Като взеха предвид това, че между Администратора и Обработващия е сключен **Договор за извършване на независим финансов одит № ……. / …….. г.**, наричан по-нататък **„основният договор“**.

Като взеха предвид това, че при изпълнението на основния договор Обработващият ще извършва от името на Администратора операции по обработване на лични данни.

Като взеха предвид това, че като част от договорните им отношения се задължават да се съобразят с приложимите разпоредби за обработка на лични данни и по-специално с Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета (Общ регламент относно защита на данните).

Като взеха предвид това, че целта на настоящото споразумение е да се определят условията, при които Обработващият се задължава да извършва от името на Администратора операциите по обработка на данни, дефинирани и конкретизирани по-долу.

Се сключи настоящото Споразумение за следното:

I. ОПИСАНИЕ И УСЛОВИЯ НА ОБРАБОТКАТА

Чл. 1. (1) Обработващият извършва операции по обработка на данни от името на Администратора за предоставяне на следната услуга / извършване на следните дейности:

а) извършване на проверка, и при наличие на условия – заверка на годишния индивидуален и консолидиран финансов отчет на Администратора към 31.12.2024 г., в съответствие с изискванията на Закона за независимия финансов одит и изразяването на сигурност по устойчивостта, Закона за счетоводството, Регламент /ЕС/№537/2014г. и приложимите одиторски стандарти;

б) изготвяне и предаване на Администратора на окончателни одиторски доклади за годишния индивидуален и консолидиран финансов отчет към 31.12.2024 г. на „Холдинг БДЖ” ЕАД, на български език, в електронен вид и на хартиен носител;

в) предаване на Администратора, в превод на английски език, на хартиен носител, на одиторски доклади за годишния индивидуален и консолидиран финансов отчет към

31.12.2024 г. на „Холдинг БДЖ” ЕАД, както и включените към тях пълен комплект от документи, съгласно действащата нормативна уредба;

г) изготвяне на допълнителни доклади към изготвените одиторски доклади за Одитния комитет на „Холдинг БДЖ” ЕАД.

(2) Характерът на дейността по обработката на лични данни е: достъп до базите с лични данни, използвани в „Холдинг БДЖ” ЕАД и/или получени от Администратора документи, справки, извлечения и др. необходими за осъществяване на услугата, посочена в ал.1 на настоящия член.

(3) Категориите лични данни, които могат да бъдат обработвани са:
имена, единен граждански номер, адрес, телефон, електронна поща, длъжност и/или трудово възнаграждение на служители на Администратора, номер на банкова сметка на физически лица и др. (поотделно или в съвкупност).

(4) Категориите субекти, на които ще се обработват лични данни са:
служители, клиенти или доставчици на „Холдинг БДЖ” ЕАД.

Чл. 2. Обработващият извършва операциите по обработка в съответствие с разпоредбите на Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. относно защита на данните на физическите лица, приложимото национално законодателство, своите и тези на Администратора: Вътрешните правила / Политики за защита на личните данни, процедури и други.

Чл. 3. (1) При изпълнението на основния договор, Обработващият обработва лични данни на Администратора единствено с цел изпълнение на предвидените в него дейности, съгласно уговорения предмет.

(2) Ако Обработващият определи самостоятелно целите и средствата за обработка на личните данни, предоставени му от Администратора, Обработващият се счита за Администратор по отношение на тази допълнителна обработка.

Чл. 4. Всички съобщения, указания и нареждане на Администратора във връзка с обработката на лични данни се извършват в писмена форма.

Чл. 5. (1) Обработващият е длъжен да поддържа регистър на дейностите по обработка, извършвани от името на Администратора.

(2) Регистърът по ал.1 следва да съдържа най – малко информация за длъжностното лице по защита на данните, ако е приложимо, категориите на обработка, предаване на лични данни на трета държава или международна организация , ако е приложимо, общо описание на техническите и организационни мерки.

Чл. 6. Обработващият не обработва лични данни на Администратора, нито разрешава на оторизиран подизпълнител да обработва личните данни на Администратора в трета страна или международна организация, освен ако тази обработка не е предварително одобрена от Администратора, чрез изменение на това Споразумение.

Чл. 7. Обработващият обработва предоставените му лични данни от името на Администратора при спазване на конфиденциалността, политиките за поверителност на Администратора и другите условия, уговорени в настоящето споразумение.

Чл. 8. Обработващият носи пълна отговорност за всички вреди, настъпили за Администратора, които са пряка и непосредствена последица от пълно неизпълнение, частично или забавено изпълнение на задълженията по настоящото Споразумение.

II. ЗАЩИТА НА ЛИЧНИТЕ ДАННИ ОТ ОБРАБОТВАЩИЯ

Чл. 9. (1) Обработващият се задължава да спазва всички организационни и технически мерки за защита на личните данни подробно описани във Вътрешните правила /

Политики за защита на личните данни на Администратора.

(2) Обработващият се задължава да предостави информация за съответствие на обработката с изискванията на Администратора, съгласно Карта за съответствие на обработката (***Приложение - КС*** към настоящото Споразумение).

(3) Обработващият предприема необходимите действия, за да гарантира, че достъпът до личните данни на Администратора е ограничен до лицата, които имат нужда от достъп тях, за да изпълнят служебните си или договорни задължения (прилагане на принципа „Необходимост да знае").

(4) Обработващият гарантира, че всички лица, които обработват личните данни под негово ръководство:

а) са информирани за поверителния характер на личните данни на Администратора и са запознати със задълженията на Обработващия съгласно настоящото Споразумение;

б) са запознати с изискванията на нормативната уредба за защитата на личните данни;

в) са поели задължение за поверителност, освен ако не са задължени да спазват поверителност във връзка с професионалните им и/или законови изисквания;

г) извършват обработката само по начина, определен от Обработващия.

Чл. 10. (1) Обработващият предприема необходимите мерки, за да гарантира сигурността на обработваните от него данни.

(2) При определяне на необходимите мерки за защита, Обработващият взема предвид минимум следните фактори:

а) състоянието и развитието на технологиите;

б) разходите по прилагане на определените мерки;

в) обхвата, контекста и целите на обработка;

г) рисковете с различна вероятност и тежест за правата и свободите на физическите лица, по-конкретно рисковете от случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или достъп до прехвърлени, съхранявани или обработени по друг начин лични данни.

(3) Предприетите мерки могат да включват, но не само (изброяването не е изчерпателно):

а) способност да се гарантира непрекъснатата поверителност, цялост, достъпност и устойчивост на системите и услугите за обработка;

б) възможност за своевременно възстановяване на наличността и достъпа до лични данни на администратора в случай на физически или технически инцидент;

в) осигурени редовно тестване, оценка и оценка на ефективността на техническите и организационните мерки за гарантиране на сигурността на обработката;

г) псевдонимизиране и криптиране.

(4) За доказване на предприетите мерки, Обработващият предоставя на Администратора съответната документация.

(5) Обработващият може да предприеме допълнителни мерки по своя преценка, ако такива са необходими за гарантиране на сигурността на обработваните данни.

III. ОБРАБОТВАНЕ НА ДАННИТЕ ОТ ПОДИЗПЪЛНИТЕЛ ПО ВЪЗЛАГАНЕ ОТ ОБРАБОТВАЩИЯ

Чл. 11. (1) Обработващият може да превъзлага обработката на данните на Администратора, само на лица (подизпълнители), които осигуряват адекватни технически и организационни мерки за сигурност на данните.

(2) Преди да ангажира подизпълнител, Обработващият трябва да:

а) предостави на Администратора пълна информация за обработката, която възнамерява да възложи на съответния подизпълнител;

б) извърши надлежна проверка за всеки подизпълнител, за да се гарантира, че той може да осигури нужното ниво на защита на личните данни на Администратора, включително, достатъчни гаранции за прилагане на подходящи технически и организационни мерки по такъв начин, че обработването да отговаря на изискванията, определени с настоящото споразумение и приложимата уредба на защита на данните.

в) поиска писмено съгласието на Администратора за ангажирането на подизпълнител. Администраторът може да откаже възлагането на обработка от определени лица.

(2) Обработващият е отговорен за всяко неизпълнение на задълженията във връзка с обработката на лични данни на Администратора, включително, когато неизпълнението е от подизпълнителя.

IV. РЕАЛИЗИРАНЕ НА ПРАВАТА НА СУБЕКТИТЕ НА ДАННИ

Чл. 12. (1) Като оцени естеството на обработката, Обработващият подпомага Администратора при изпълнение на задълженията на Администратора във връзка с исканията за упражняване на права от субектите на данни.

(2) Обработващият е задължен да уведоми Администратора в разумен срок, но не по – късно от 24 часа, в случай на постъпило при него или при негов подизпълнител искане за упражняване на права от субект на данни, от надзорния орган и / или друг компетентен орган, свързано с личните данни на администратора.

(3) Обработващият предоставя всички данни за обработката, поискани от Администратора в рамките на разумен срок определен от Администратора. Разумността на срока се преценява с оглед естеството и обема на исканите данни, но не може да бъде по – дълъг от 15 дни.

(4) Обработващият съдейства на Администратора, включително чрез извършване на допълнителни действия, поискани от Администратора, за да може последният да отговори на отправените до него жалби, съобщения или искания.

V. ЗАДЪЛЖЕНИЯ ПРИ НАРУШАВАНЕ НА СИГУРНОСТТА НА ЛИЧНИТЕ ДАННИ

Чл. 13. (1) Обработващият уведомява Администратора без неоснователно забавяне, но не по-късно от изтичането на 24 часа, след като е узнал или подозира за нарушение на сигурността на личните данни.

(2) Обработващият е задължен да предостави на Администратора необходимата информация за изпълнение на задължението на Администратора да съобщи за нарушението на сигурността на личните данни на надзорния орган (Комисия за защита на личните данни).

(3) Уведомяването по ал. 1, включва като минимум описание на:

а) естеството на нарушението на сигурността на личните данни;

б) категориите и броя на засегнатите лица;

в) категориите и броя на засегнатите записи на лични данни;

г) прогнозния риск и вероятните последици от нарушаването на сигурността на личните данни;

д) мерките, предприети или предложени за справяне с нарушаването на сигурността на личните данни;

е) името и данните за контакт на длъжностното лица по защита на данните или на

друго лице, от което може да бъде получена повече информация.

(4) В случай на нарушаване на сигурността на личните данни Обработващият няма да информира трета страна, без преди това да получи предварителното писмено съгласие на Администратора, освен ако информирането се извършва въз основа на закон.

Чл. 14. (1) Обработващият се задължава да прилага относимите норми на Регламент 2016/679 и ЗЗЛД в случай на нарушение на сигурността на личните данни, като предоставя на Администратора информация за предприетите от него действия за ограничаване на вредите от нарушението.

(2) Информацията по ал.1 се предоставя на Администратора в срок до 48 часа от узнаването или възникването на съмнение за нарушение на сигурността на личните данни.

VI. ОЦЕНКА НА ВЪЗДЕЙСТВИЕТО ВЪРХУ ЗАЩИТА НА ДАННИТЕ

Чл. 15. Обработващият предоставя помощ на Администратора при извършване на оценки на въздействието върху защитата на личните данни, когато такива се извършват от Администратора и в случай, че засягат обработката, извършвана от Обработващия.

VII. ИЗТРИВАНЕ ИЛИ ВРЪЩАНЕ НА ЛИЧНИ ДАННИ НА АДМИНИСТРАТОРА

Чл. 16. (1) В рамките на 7 (седем) календарни дни от прекратяване на обработката на лични данни на Администратора от Обработващия или от прекратяване на основния договор, Обработващият предприема едно или няколко от посочените действия, определени допълнително в писмен вид от Администратора:

а) връща данните, обективирани на хартиен носител и унищожава по начин, който не позволява възстановяването, всички копия, независимо от формата, в която са налични, направени във връзка с обработката;

б) връща пълно копие от всички лични данни на Администратора, обработвани в електронна форма, чрез защитено прехвърляне на файлове в такъв формат, какъвто му е посочен от Администратора и сигурно изтрива всички други копия от личните данни на Администратора, обработвани от Обработващия или оторизиран от него подизпълнител;

в) изтрива сигурно всички копия от личните данни на Администратора, обработвани от Обработващия или оторизиран от него подизпълнител.

(2) Обработващия предоставя доказателства на Администратора, че е спазил напълно изискването за изтриване на наличните у него данни.

VIII. ИЗВЪРШВАНЕ НА ОДИТ

Чл. 17. (1) Обработващият предоставя при поискване от Администратора цялата информация, необходима за доказване на съответствие с това споразумение и с изискванията на националното и европейското законодателство за защита на личните данни.

(2) Обработващият позволява и подпомага извършването на одитите от Администратора или на друг одитор по възлагане от Администратора.

(3) При поискан от Администраторът одит Обработващият е длъжен да:

а) предостави на Администратора или на друг одитор, упълномощен от администратора достъп до всички помещения, в които се извършва обработката на данните

на Администратора;

б) позволи проверката, включително копирането на всички налични масиви и системи, чрез които се извършва обработката, за да може Администраторът да се увери, че са спазени разпоредбите на това Споразумение.

За изпълнение на настоящото Споразумение страните определят следните лица и данни за контакт:

За Администратора: …… – длъжностно лице по защита на личните данни, тел.: (+359) ……., електронна поща: ……..;

За Обработващия: ……., тел. ……, електронна поща: …….

Настоящото Споразумение влиза в сила от ……. и се прекратява с прекратяването на основния договор.

За Администратора:

…….
инж. Георги Друмев
Изпълнителен директор

За Обработващия:

…….……
……

КАРТА ЗА СЪОТВЕТСТВИЕ НА ОБРАБОТКАТА НА ЛИЧНИ ДАННИ

1. Имате ли разработени, включително документирани процедури за изпълнение на искания от администратора:
   a. За коригиране на обработвани от Вас лични данни:
      ☐ Да

      ☐ Не

   b. За изтриване на лични данни:
      ☐ Да

      ☐ Не

   c. За ограничаване на обработването само до съхранение:
      ☐ Да

      ☐ Не

   d. Можете ли да осигурите преносимост на личните данни, обработвани от името на Администратора
      ☐ Да

      ☐ Не

2. Имате процедура/ред за информиране на администратора, в случай на възлагане на част от дейностите по обработка на друг обработващ?
   ☐ Да

   ☐ Не

3. Можете ли да гарантирате, че възлагате част от дейностите по обработка на друг обработващ на лични данни от администратора, само ако осигурява достатъчно гаранции за прилагане на подходящи технически и организационни мерки по такъв начин, че обработката да гарантира защитата на личните данни, получени от администратора?
   ☐ Да

   ☐ Не

4. Можете ли да гарантирате, че всички служители (вътрешни и външни), които работят с лични данни, предоставени от администратора, са ангажирани със защитата на данните и спазват изискване за поверителност на данните?
   ☐ Да

   ☐ Не

5. Провеждате ли обучение за служителите, работещи с лични данни, предоставени от администратора?
   ☐ Да

☐ Не

Ако да – с каква периодичност са тези обучения.

……
……
……
……
……
……
……

6. Налице ли е общ преглед на всички бизнес процеси / информационни системи, обработващи лични данни, предоставени от администратора?
   ☐ Да

   ☐ Не

7. Налични ли са следните технически и организационни мерки по отношение на личните данни на администратора:
   a. Псевдонимация и криптиране вследствие на критичността на личните данни?
      ☐ Да

      ☐ Не

Ако да, моля да посочите в какви случаи ги прилагате

……
……
……
……
……

   b. Възможност да се гарантира непрекъснатата поверителност, целостта, наличността и устойчивостта на обработващите системи и услуги?
      ☐ Да

      ☐ Не

Ако да, моля да посочите по какъв начин се осигуряват
……
……
……
……
…….....

   c. Възстановяване и осигуряване на своевременен достъп до лични данни в случай на физически или технически инциденти?
      ☐ Да

      ☐ Не

Ако да, моля да посочите как гарантирате възстановяването и осигуряването на своевременен достъп

……
……
……
……
……

d. Процеси за редовно тестване, оценка и оценка на ефективността на техническите и организационните мерки за гарантиране на сигурността на обработката?
☐ Да

☐ Не

8. Имате ли установена процедура за действие, когато има нарушение на сигурността, което засяга личните данни, предоставени от администратора?
☐ Да

☐ Не

a. Налице ли е изискване за уведомяване на администратора веднага щом установите нарушението?
☐ Да

☐ Не

b. Налице ли е изискване е за документиране на всички факти, свързани с нарушението на личните данни, неговите последици и предприетите коригиращи действия?
☐ Да

☐ Не

c. Налице ли е изискване за съхраняване на доказателства, необходими за доказване пред контролните и съдебните органи?
☐ Да

☐ Не

9. Имате ли определено длъжностно лице по защита на личните данни.
☐ Да

☐ Не

Ако да, моля да посочите имената и данните за контакт с него

……
……
……
……

За Обработващия:

…….

……