ПРАВИЛА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

DATA PROTECTION RULES

ГЛАВА I. ОБЩИ ПОЛОЖЕНИЯ

CHAPTER I. GENERAL PROVISIONS

Чл. 1. С настоящите правила за защита на личните данни се определят политиката и необходимите технически и организационни мерки за защита на личните данни на клиентите, контрагентите и служителите на „МаркетВижън Файнънс“ ООД (**Дружеството**) съгласно Регламент (ЕС) № 2016/679 на Европейския Парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни (**ОРЗД**), Закона за защита на личните данни (**ЗЗЛД**) и всички други приложими подзаконови нормативни актове.

Art. 1. These Rules on personal data protection determine the policy and the necessary technical and organisational measures for the protection of personal data of clients, contractors and employees of MarketVision Finance OOD **(Company)**, according to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data (**GDPR**), the Personal Data Protection Act (**PDPA**) and all other applicable regulations.

Чл. 2. (1) Настоящите правила са задължителни за всички служители на Дружеството и са насочени към осигуряване на адекватно ниво на защита на поддържаните регистри с лични данни от случайно или незаконно унищожаване, от случайна загуба, от неправомерен достъп, изменение или разпространение, както и от други незаконни форми на обработване.

Art. 2. (1) These Rules are mandatory for all employees of the Company and are aimed at ensuring an adequate level of protection of the maintained registers with personal data from accidental or illegal destruction, accidental loss, illegal access, modification, or distribution, as well as from other illegal forms of processing.

(2) Правилата информират служителите на Дружеството за правата им като субекти на лични данни съгласно ОРЗД. С правилата Дружеството цели също така да приложи мерки, които отговарят по-специално на принципите за защита на данните на етапа на проектирането и защита на данните по подразбиране, които мерки се изразяват, inter alia, в свеждане до минимум на обработването на лични данни, псевдонимизиране на лични данни на възможно най-ранен етап, прозрачност по отношение на функциите и обработването на лични данни, създаване на възможност за субекта на данни за достъп до обработваните данни, възможност за Дружеството да създава и подобрява елементите на сигурността.

(2) These Rules shall inform the employees of the Company about their rights as subjects of personal data according to GDPR. With these Rules, the Company also aims to implement measures that comply in particular with the principles of data protection at the design stage and data protection by default, which measures are, inter alia, to minimise the processing of personal data, pseudonymization of personal data at the earliest possible stage, transparency regarding the functions and processing of personal data, creation of an opportunity for the data subject to access the processed data, opportunity for the Company to create and improve the security elements.

Чл. 3. Всички обработвани лични данни ще бъдат третирани като строго поверителни. Основните

Art. 3. All processed personal data shall be treated as strictly confidential. The main principles that are applied by the Company in the processing of personal data are:

принципи, които се прилагат от Дружеството при обработването на лични данни са:

1. законосъобразност, добросъвестност и прозрачност през целия процес на обработване на лични данни;

1. legality, good faith, and transparency throughout the process of personal data processing;

2. ограничение на целите - личните данни, които Дружеството обработва, се събират за конкретни, изрично указани и легитимни цели и не се обработват по начин, несъвместим с тези цели;

2. restriction of the purposes - the personal data, which the Company processes, are collected for specific, expressly indicated, and legitimate purposes and are not processed in a way, incompatible with these purposes;

3. Дружеството свежда до минимум личните данни, които обработва, и те се ограничават до такива, необходими за целите, за които се обработват, без да изисква излишни данни;

3. the Company shall minimise the personal data it processes, and it shall be limited to those necessary for the purposes for which they are processed, without requiring redundant data;

4. точност при обработването – Дружеството поддържа в актуален вид личните данни, които обработва, и предприема всички разумни мерки, за да се гарантира своевременното изтриване или коригиране на неточни лични данни, като се имат предвид целите, за които те се обработват;

4. accuracy in processing - the Company maintains up-to-date personal data, which it processes and takes all reasonable measures to ensure the timely deletion or correction of inaccurate personal data, considering the purposes for which they are processed;

5. ограничение на съхранението – личните данни се съхраняват във форма, която позволява идентифицирането на субекта на данните за период, не по-дълъг от необходимото за целите, за които се обработват, като се вземат предвид всички приложими нормативни срокове и разпоредби, които Дружеството трябва да спазва;

5. restriction of storage - personal data are stored in a form that allows the identification of the data subject for a period not longer than necessary for the purposes for which they are processed, considering all applicable regulations and provisions that the Company must comply;

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

6. integrity and confidentiality - personal data shall be processed in a way that ensures an appropriate level of security, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage, by applying appropriate technical or organizational measures.

Чл. 4. Съгласно настоящите правила:

Art. 4. According to these Rules:

1. *„длъжностно лице по защита на личните данни”* (**ДЛЗЛД**) е физическо лице, притежаващо необходимата компетентност и професионални качества, което е назначено от Дружеството във връзка със спазване на приложимото

1. *“Data Protection Officer”* (**DPO**) shall mean a natural person with the necessary competence and professional qualities, who is appointed by the Company in connection with the observance of the applicable legislation and

законодателство и контрол при осигуряване на необходимите технически и организационни мерки за защита на личните данни;

control in ensuring the necessary technical and organisational measures for personal data protection;

2. *„лични данни”* означава всяка информация, отнасяща се до физическо лице, което е идентифицирано или може да бъде идентифицирано пряко или непряко по-специално чрез идентификатор като име, идентификационен номер, данни за местонахождение, телефон или по един или повече специфични признаци;

2. *“personal data”* shall mean any information relating to a natural person which is or can be identified, directly or indirectly, in particular by means of an identifier such as name, identification number, location data, telephone number or one or more specific features;

3. *„обработване на лични данни”* е всяко действие или съвкупност от действия, които могат да се извършват по отношение на личните данни с автоматични или други средства, като събиране, записване, организиране, структуриране, съхраняване, адаптиране, извличане, употреба, разпространяване, комбиниране, ограничаване, изтриване или унищожаване;

3. *“processing of personal data”* shall mean any action or set of actions that can be performed on personal data by automatic or other means, such as collection, recording, organisation, structuring, storage, adaptation, retrieval, use, distribution, combining, restricting, deleting or destroying;

4. *„регистър на лични данни”* е всеки структуриран набор от лични данни, достъпът до който се осъществява съгласно определени критерии.

4. "*Personal Data Register*" shall mean any structured set of personal data, the access to which is carried out according to certain criteria.

ГЛАВА II. ОБЩО ОПИСАНИЕ НА ПОДДЪРЖАНИТЕ РЕГИСТРИ. КАТЕГОРИИ ЛИЧНИ ДАННИ И ОСНОВАНИЕ ЗА ОБРАБОТВАНЕ

CHAPTER II. GENERAL DESCRIPTION OF THE MAINTAINED REGISTERS. CATEGORIES OF PERSONAL DATA AND GROUNDS FOR PROCESSING

Чл. 5. Дружеството въвежда подходящи технически и организационни мерки, за да се гарантира, че по подразбиране се обработват само лични данни, които са необходими за всяка конкретна цел на обработването. Това задължение се отнася до обема на събраните лични данни, степента на обработването, периода на съхраняването им и тяхната достъпност. По-специално, подобни мерки гарантират, че по подразбиране без намеса от страна на физическото лице личните данни не са достъпни за неограничен брой физически лица.

Art. 5. The Company shall put in place appropriate technical and organisational measures to ensure that, by default, only personal data that is necessary for each specific purpose of processing are processed. This obligation relates to the volume of personal data collected, the degree of processing, the period of their storage and their availability. In particular, such measures shall ensure that, by default, personal data is not available to an unlimited number of individuals without the intervention of the individual.

Чл. 6. В Дружеството са обособени четири регистъра за лични данни в зависимост от целите на обработка:

Art. 6. The Company has four Personal Data Registers depending on the purposes of processing:

1. Регистър „Клиенти‘‘;

1. Clients' Register;

2. Регистър „Контрагенти”;

3. Регистър „Доставчици‘‘;

4. Регистър „Служители”.

2. Contractors' Register;

3. Suppliers' Register;

4. Employees' Register.

Регистър „Клиенти‘‘

Clients’ Register

чл. 7. В Регистър „Клиенти” се набират и съхраняват лични данни на клиентите и инвеститори в АИФ - физически лица. Регистърът се води по електронен път и включва цялата изискуема информация за клиентите на основание Закона за мерките срещу изпирането на пари (**ЗМИП**), Закона за дейността на колективните инвестиционни схеми и на други предприятия за колективно инвестиране (**ЗДКИСДПКИ**), както и подзаконовите нормативни актове по тяхното прилагане и вътрешните актове на Дружеството.

Art. 7. The personal data of clients and investors in AIF - individuals is collected and stored in the Clients’ Register. The register is kept electronically and includes all the required information for the clients, on the basis of the Prevention of Money Laundering Act (**PMLA**), the Activity of Collective Investment Schemes and Other Collective Investment Enterprises Act (**ACISOCIEA**), as well as the bylaws on their application and the internal acts of the Company.

Чл. 8. (1) Личните данни, които клиентите предоставят преди или при сключване на договор, може да включват:

Art. 8. (1) The personal data, which the clients provide before or at the moment of entering into a contract, may include:

1. имейл адрес;

2. име, презиме и фамилия;

3. държава на пребиваване;

4. телефонен номер за връзка;

5. адрес по лична карта или друг документ за идентификация;

6. настоящ адрес (град; пощенски код; държава);

7. ЕГН/данъчен номер;

8. националност;

9. информация дали физическото лице е политически изявена личност или е пряко свързано с политически изявена личност;

10. информация относно образование, финансов опит и/или професионален опит.

1. e-mail address;

2. name, middle name and surname;

3. country of residence;

4. telephone number for contact;

5. address by ID card or other identification document;

6. current address (city; postal code; country);

7. ID/Tax number;

8. nationality;

9. information whether the natural person is a politically prominent person or whether he/she is directly connected with a politically prominent person;

10. information regarding education, financial experience and/or professional experience.

(2) Личните данни се събират чрез попълване на формуляр на сайта на Дружеството или на място в офис. Гореописаните лични данни се събират, за да може да се извърши идентификация на физическите лица, която Дружеството е задължено да извърши по закон, както и за допълнителна сигурност на самите физически лица.

(2) The personal data is collected by filling in a form on the website of the Company or on the spot in an office. The above-described personal data is collected in order to be able to identify individuals, which the Company is obliged to perform by law, as well as for additional security of the individuals themselves.

(3) Събраните лични данни от Регистър „Клиенти‘‘ се използват за следните цели:

(3) The personal data collected by the Clients' Register shall be used for the following purposes:

1. предоставяне на инвестиционни услуги – 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. Дружеството не може да сключи договор с клиент без надлежно да го идентифицира и съответно личните данни са необходими за индивидуализиране на договорните правоотношения, воденето на счетоводна отчетност относно притежаваните от клиента дялове, внасяне или теглене на средства и др.;

1. provision of investment services - the processing is necessary for the performance of a contract to which the data subject is a party or for taking steps at the request of the data subject before the conclusion of the contract. The company cannot conclude a contract with a client without properly identifying it and accordingly the personal data are necessary for individualization of the contractual legal relations, keeping accounting records regarding the shares held by the client, depositing or withdrawing funds, etc.;

2. спазване на законово задължение, което се прилага спрямо Дружеството;

2. compliance with a legal obligation that applies to the Company;

3. обработването на лични данни е необходимо за целите на законните интереси, преследвани от Дружеството;

3. the processing of personal data is necessary for the purposes of the legal interests pursued by the Company;

4. маркетинг цели – в рамките на даденото от клиента съгласие (ако е приложимо).

4. marketing purposes - within the consent given by the client (if applicable).

Чл. 9. В съответствие с чл. 30 ОРЗД, Дружеството създава и поддържа Регистър „Клиенти‘‘. Ръководителят на отдел „Нормативно съответствие‘‘ отговаря за воденето, поддържането и съхранението на всички регистри на Дружеството.

Art. 9. In accordance with Art. 30 GDPR, the Company creates and maintains the Clients' Register. The Head of the Regulatory Compliance Department is responsible for keeping, maintaining and storing all registers of the Company.

Чл. 10. Достъпът до личните данни е оторизиран и е възможен само за тези служители на Дружеството, за които това е необходимо за изпълнение на служебните им задължения.

Art. 10. The access to the personal data is authorized and is possible only for those employees of the Company, for whom this is necessary for the performance of their official duties.

Чл. 11. Копирането на документи и/или каквато и да е информация, съдържащи лични данни на електронен или хартиен носител, е забранено. Копирането на

Art. 11. The copying of documents and/or any information containing personal data on electronic media is prohibited. The copy of documents on paper and the use

документи на хартиен носител или използването на записващи устройства, които позволяват копирането на документи на електронен носител, е позволено само за целите на изпълнение на служебни задължения, като например изпращане на данни към административни и контролни органи (КФН, НАП, НОИ) посредством електронен подпис.

of recording devices that allow the copying of documents on electronic media is allowed only for the purposes of performing official duties, such as sending data to administrative and control bodies (FSC, NRA, NSSI) by electronic signature.

Регистър „Доставчици”

Suppliers' Register

Чл. 12. Дружеството сключва договори за доставка на стоки и услуги с различни доставчици за целите на изпълнение на предмета на своята дейност. В този регистър се набират и съхраняват данни за доставчиците на стоки и услуги на Дружеството. В случаите, когато Дружеството предоставя лични данни на свои доставчици, Дружеството осигурява спазване на ОРЗД чрез подписване на допълнителни споразумения към съществуващите договорни отношения.

Art. 12. The Company enters into contracts for supply of goods and services with various suppliers for the purposes of performing the objects of its activities. This register collects and stores data on the suppliers of goods and services of the Company. In the cases when the Company provides personal data to its suppliers, the Company ensures compliance with the GDPR by signing additional agreements to the existing contractual relations.

Чл. 13. Регистър „Доставчици” се поддържа на електронен носител и включва идентифициращи данни за съответния контрагент (като име, ЕИК/ЕГН, адрес за кореспонденция, имейл на лице за контакт, телефон, предмет на договора, срок за изпълнение/доставка). В регистъра се съдържат и лични данни като трите имена на съответните физически лица, ЕГН, телефон, имейл и адрес за кореспонденция за доставчиците на Дружеството, които са физически лица, с цел тяхната идентификация и спазване на приложимото данъчно законодателство. Такива доставчици са ограничен кръг от физически лица и са изключение в ежедневната практика на Дружеството.

Art. 13. The Suppliers' Register is maintained in electronic form and includes identifying data for the respective contractor (such as name, UIC/ID, address for correspondence, e-mail of contact person, telephone, subject of the contract, deadline for delivery). The register also contains personal data such as the three names of the respective individuals, ID, telephone, email and mailing address for the Company's suppliers who are individuals, in order to identify them and comply with applicable tax legislation. Such suppliers are a limited number of individuals and are an exception in the daily practice of the Company.

Чл. 14. Събраните лични данни се използват за следните цели:

Art. 14. The collected personal data shall be used for the following purposes:

1. индивидуализиране на договорните правоотношения - обработването е необходимо за изпълнението на договор, по който субектът на данни (физическото лице) е страна;

1. identification of contractual relations - the processing is necessary for the performance of a contract to which the data subject (the natural person) is a party;

2. спазване на законово задължение, което се прилага спрямо Дружеството, а именно - изпълнение

2. compliance with a legal obligation that applies to the Company, namely - compliance with regulatory

на нормативните изисквания съгласно Закона за корпоративното подоходно облагане, Закона за данъците върху доходите на физическите лица, Закона за данък върху добавената стойност, Закона за счетоводството, ЗДКИСДПКИ, Закона за мерките срещу изпирането на пари и други законови и подзаконови нормативни актове;

requirements under the Corporate Income Tax Act, the Personal Income Tax Act, the Value Added Tax Act, the Accounting Act, the CIS Act, the Act for measures against money laundering and other laws and regulations;

3. използване на събраните данни за служебни цели, свързани със съществуването, изменението и прекратяването на договорните правоотношения с доставчиците, воденето на счетоводна отчетност и др.

3. use of the collected data for official purposes, related to the existence, the amendment and the termination of the contractual legal relations with the suppliers, the keeping of accounting, etc.

Регистър „Контрагенти”

Contractors' Register

Чл. 15. В съответствие с чл. 30 ОРЗД, Дружеството създава и поддържа Регистър „Контрагенти”.

Art. 15. Pursuant to art. 30 GDPR, the Company creates and maintains Contractors' Register.

Чл. 16. Достъпът до личните данни в Регистър „Контрагенти” е оторизиран и е възможен само за тези служители на Дружеството, за които това е необходимо за изпълнение на служебните им задължения.

Art. 16. The access to the personal data in the Contractors' Register is authorised and is possible only for these employees of the Company, for whom this is necessary for the performance of their official duties.

Чл. 17. Копирането на документи и/или каквато и да е информация, съдържащи лични данни на електронен или хартиен носител носител, е забранено. Копирането на документи на хартиен носител или използването на записващи устройства, които позволяват копирането на документи на електронен носител, е позволено само за целите на изпълнение на служебни задължения, като например изпращане на данни към административни и контролни органи (КФН, НАП, НОИ) посредством електронен подпис.

Art. 17. The copying of documents and/or any information containing personal data on electronic media is prohibited. The copy of documents on paper and the use of recording devices that allow the copying of documents on electronic media is allowed only for the purposes of performing official duties, such as sending data to administrative and control bodies (FSC, NRA, NSSI) by electronic signature.

Чл. 18. Дружеството прилага същите правила на работа в случай на постъпили молби от контрагенти във връзка с упражняване на правата им съгласно ОРЗД, които се съдържат в Приложение № 1 към настоящите правила.

Art. 18. The Company applies the same rules of operation in case of received requests from contractors in connection with the exercise of their rights under the GDPR, which are contained in Schedule 1 to these Rules.

Регистър „Служители”

Employees' Register

Чл. 19. Дружеството води отчетност за физически лица, намиращи се в трудови, приравнени на трудови и граждански правоотношения с Дружеството, бивши служители, както и кандидати за работа. За тази цел,

Art. 19. The Company keeps records for natural persons who are in employment, equated to employment and civil legal relations with the Company, former employees, as well as job candidates. For this purpose, in accordance

в съответствие с чл. 30 ОРЗД, Дружеството създава и поддържа Регистър „Служители‘‘.

Чл. 20. Личните данни на всички служители на Дружеството се обработват на основание Кодекса на труда, Кодекса на социалното осигуряване и приложимите подзаконови нормативни актове. Данните се въвеждат в специализиран софтуер и съдържат:

1. три имена, ЕГН, постоянен адрес, телефон, имейл;

2. образование, специалност, място на придобиване на образованието, номер на диплома и дата на издаване, научна степен (ако е приложимо);

3. трудов стаж, сектори, в които лицето е работило, допълнителна квалификация;

4. болнични листове – номер на болничен лист; име на служител; адрес; причина за временната нетрудоспособност; срок на болничния лист;

5. други документи и информация съгласно приложимото законодателство.

Чл. 21. Събраните лични данни се използват за следните цели:

1. индивидуализиране и сключване на трудови и граждански правоотношения;

2. изпълнение на нормативните изисквания на Кодекса на труда, Кодекса за социално осигуряване, Закона за счетоводството, Закона за данъците върху доходите на физическите лица и др.;

3. използване на събраните данни за служебни цели, свързани със съществуването, изменението и прекратяването на трудовите и гражданските правоотношения, воденето на счетоводна отчетност относно възнагражденията на посочените по-горе лица и др.

Работа и достъп до лични данни от Регистър „Служители‘‘

with Art. 30 GDPR, the Company creates and maintains the Employees' Register.

Art. 20. The personal data of all employees of the Company are processed on the basis of the Labor Code, the Social Security Code and the applicable by-laws. The data is entered in specialised software, and contain:

1. three names, PIN, permanent address, telephone, e-mail;

2. education, specialty, place of acquisition of education, diploma number and date of issue, scientific degree (if applicable);

3. length of service, sectors in which the person has worked, additional qualification;

4. sick leaves - number of sick leave; name of employee; address; reason for temporary incapacity for work; term of the sick leave;

5. other documents and information according to the applicable legislation.

Art. 21. The collected personal data shall be used for the following purposes:

1. individualization and conclusion of labour and civil legal relations;

2. fulfilment of the normative requirements of the Labor Code, the Social Insurance Code, the Accounting Act, the Personal Income Tax Act, etc .;

3. use of the collected data for official purposes, related to the existence, change and termination of the labor and civil legal relations, keeping the accounting records regarding the remunerations of the above-mentioned persons, etc.

Work and access to personal data from the Employees' Register

Чл. 22. Личните данни от Регистър „Служители” се събират, обработват и съхраняват от служители от отдел „Счетоводство” на хартиен и електронен носител, като за всеки служител по трудово правоотношение се съставя и води трудово досие.

Art. 22. The personal data from the Employees' Register are collected, processed and stored by employees of the Accounting Department on paper and electronic media, and for each employee a labour file is compiled and maintained.

Чл. 23. Данните за лицата, наети по граждански договори, се събират, обработват и съхраняват от отдел „Счетоводство” на хартиен и електронен носител.

Art. 23. The data of the persons employed under civil contracts shall be collected, processed and stored by the Accounting Department on paper and electronic media.

Чл. 24. Процедурата за работа при постъпили молби от служители на Дружеството във връзка с упражняване на правата им съгласно ОРЗД се съдържа в Приложение № 2 към настоящите правила.

Art. 24. Procedure for work in case of received requests from employees of the Company in connection with the exercise of their rights under the GDPR, are contained in Schedule 2 to these Rules.

ГЛАВА III. ПРАВА НА СЛУЖИТЕЛИТЕ НА ДРУЖЕСТВОТО ВЪВ ВРЪЗКА С ОБРАБОТВАНИТЕ ЛИЧНИ ДАННИ

CHAPTER III. RIGHTS OF THE EMPLOYEES OF THE COMPANY IN CONNECTION WITH THE PROCESSED PERSONAL DATA

Чл. 25. (1) С настоящите правила Дружеството информира своите служители за правата им във връзка с обработваните лични данни, както следва:

Art. 25. (1) With these Rules the Company informs its employees about their rights in connection with the processed personal data, as follows:

1. право на достъп и информация за обработваните лични данни, както и информация какви лични данни и за каква цел се обработват, кои са получателите на данни, както и какъв е срокът на обработване;

1. right of access and information about the processed personal data, as well as information about what personal data and for what purpose are processed, who are the recipients of data, as well as what is the processing time;

2. право на коригиране на личните данни, които са неточни/неактуални;

2. right to correction of the personal data, which are inaccurate / out of date;

3. право на ограничаване обработването на лични данни, в случай че:

3. right to limit the processing of personal data, in case:

а) личните данни не са точни, като в този случай ограничаването е за срок, необходим на Дружеството да провери точността;

a) the personal data are not accurate, in which case the restriction is for a period necessary for the Company to check the accuracy;

б) обработването на личните данни е неправомерно, но служителят не желае те да бъдат изтрити, а само да бъде ограничено използването им;

b) the processing of personal data is illegal, but the employee does not want them to be deleted, but only to restrict their use;

в) Дружеството не се нуждае повече от личните данни за целите на обработването, но субектът на данни ги изисква за установяването, упражняването или защитата на правни претенции;

c) The company no longer needs the personal data for the purposes of processing, but the data subject requires them for the establishment, exercise or protection of legal claims;

г) субектът на данни е възразил срещу обработването в очакване на проверка дали законните основания на Дружеството имат преимущество пред интересите на субекта на данни.

d) the data subject has objected to the processing pending verification of whether the legal grounds of the Company take precedence over the interests of the data subject.

4. право на изтриване – служител може да поиска Дружеството да заличи личните му данни от всички системи и записи, където те се съхраняват, включително да уведоми всички трети лица/обработващи лични данни, на които е предоставил данните, освен ако Дружеството няма задължения по закон да съхранява личните данни за определен период от време.

4. right of deletion - an employee may request the Company to delete his personal data from all systems and records where they are stored, including to notify all third parties/processors of personal data to whom he has provided the data, unless the Company has obligations under law to store personal data for a certain period of time.

Това искане ще бъде удовлетворено, при условие че Дружеството няма правно задължение да съхранява тези данни и ще бъде под условие на всички давностни срокове, които е задължено да спазва в съответствие с приложимите закони и подзаконови нормативни актове.

This request will be granted, provided that the Company has no legal obligation to store this data and will be subject to all statutes of limitations, which it is obliged to comply with in accordance with applicable laws and regulations.

5. право на възражение срещу обработването на лични данни. Дружеството следва да се мотивира дали приема възражението, респ. защо продължава да обработва личните данни, ако отхвърли възражението;

5. right to object to the processing of personal data. The company should be motivated whether it accepts the objection, resp. why he continues to process personal data if he rejects the objection;

6. право на преносимост на данни – всеки настоящ или бивш служител има право, да поиска личните му данни да бъдат предадени в организиран, широко използван и пригоден за машинно четене формат на друго лице (администратор на лични данни), когато това е технически възможно;

6. right to data portability - each current or former employee has the right to request that his personal data be transmitted in an organised, widely used and machine-readable format to another person (personal data controller) where technically possible;

7. право на жалба пред компетентния надзорен орган - Комисия за защита на личните данни, адрес: гр. София 1592, бул. „Проф. Цветан Лазаров” № 2 (www.cpdp.bg).

7. right to appeal before the competent supervisory body - Commission for Personal Data Protection, having its address at 2 Tsvetan Lazarov Blvd, Sofia, 1592 (www.cpdp.bg).

(2) Когато има риск за нарушение сигурността на личните данни, Дружеството е задължено да уведоми своите служители за естеството на нарушението и какви мерки са предприети за отстраняването му, както и дали е уведомен надзорният орган за нарушението.

(2) When there is a risk for violation of the security of personal data, the Company is obliged to notify its employees of the nature of the violation and what measures have been taken for its elimination, as well as whether the supervisory body has been notified of the violation.

(3) Всеки служител има право на защита по съдебен или административен ред, в случай че правата му във връзка с личните данни са били нарушени.

(4) За да упражни което и да е от правата, изброени по-горе, и/или при въпроси, свързани с лични данни, всеки служител следва да опише искането си в писмен вид и да го адресира по имейл на следния електронен адрес: info@bgprestigefund.com.

(5) Искането трябва да съдържа:

1. име, ЕГН и адрес на заявителя;

2. описание на искането;

3. предпочитана форма за предоставяне на достъпа до личните данни;

4. подпис, дата на подаване на заявлението и адрес за кореспонденция.

(6) Дружеството разглежда заявлението за достъп и се произнася по него в 30-дневен срок от получаването на искането.

ГЛАВА IV. ДЛЪЖНОСТИ, СВЪРЗАНИ С ОБРАБОТВАНЕТО И ЗАЩИТАТА НА ЛИЧНИ ДАННИ. ПРАВА И ЗАДЪЛЖЕНИЯ

Чл. 26. Отдел „Нормативно съответствие" отговаря за защитата на личните данни и за спазването на настоящите правила. В допълнение и съгласно изискванията на ОРЗД, Дружеството назначава Длъжностно лице по защита на личните данни.

Чл. 27. При изпълнение на задълженията си отдел „Нормативно съответствие" се ръководи от разпоредбите на приложимото законодателство относно защитата на лични данни, както и от настоящите правила.

Чл. 28. Отдел „Нормативно съответствие" има следните задължения:

(3) Every employee has the right to protection by judicial or administrative order in case his rights in connection with the personal data have been violated.

(4) In order to exercise any of the rights listed above and/or in matters relating to personal data, each employee should describe his request in writing and address it by e-mail to the following email address: info@bgprestigefund.com.

(5) An application must contain:

1. name, ID and address of the applicant;

2. description of the request;

3. preferred form for providing access to personal data;

4. signature, date of submission of the application and address for correspondence.

(6) The company shall consider the application for access and shall rule on it within 30 days from the receipt of the request.

CHAPTER IV. POSITIONS RELATED TO THE PROCESSING AND PROTECTION OF PERSONAL DATA. RIGHTS AND OBLIGATIONS

Art. 26. The Regulatory Compliance Department is responsible for the protection of personal data and for compliance with these Rules. In addition and in accordance with the requirements of the GDPR, the Company appoints a Personal Data Protection Officer.

Art. 27. In the performance of its duties, the Regulatory Compliance Department shall be guided by the provisions of the applicable legislation on the protection of personal data, as well as by these Rules.

Art. 28. The Regulatory Compliance Department shall have the following obligations:

1. осигурява организацията по воденето на регистрите съгласно предвидените мерки за гарантиране на адекватна защита;

1. ensure the organisation of the keeping of the registers according to the envisaged measures for guaranteeing adequate protection;

2. упражнява непосредствен контрол върху служителите на Дружеството за спазване на изискванията за защита на личните данни;

2. exercise direct control over the employees of the Company for observance of the requirements for protection of the personal data;

3. следи за изправността и правилното функциониране на техническите и програмно-информационните ресурси;

3. monitor the serviceability and proper functioning of the technical and program-information resources;

4. следи за опитите и предотвратява такива за неразрешен достъп до базите с данни в регистрите;

4. monitor the attempts and prevent such for unauthorised access to the databases in the registers;

5. уведомява лицата, представляващи Дружеството, както и длъжностното лице по защита на личните данни, за всеки опит за неразрешен достъп до системите за сигурност, съответно за осъществен пробив в системите за сигурност, за нанесените щети /ако има такива/ и за предприетите мерки за отстраняване на проблема;

5. notify the persons representing the Company, as well as the personal data protection officer, of any attempt for unauthorised access to the security systems, respectively of a breach in the security systems, of the damages /if any/ and of the measures taken to fix the problem;

6. ежегодно провеждат прегледи относно необходимостта от обработване на данните, както и за заличаването им - за резултатите от извършени проверки се съставя протокол.

6. annually conduct inspections regarding the necessity of data processing, as well as for their deletion - a report shall be drawn up for the results of performed inspections.

Чл. 29. Отдел „Нормативно съответствие" има следните права:

Art. 29. The Regulatory Compliance Department shall have the following rights:

1. право на достъп до обработваната и съхранявана информация от регистрите;

1. right of access to the processed and stored information from the registers;

2. право да изискват съдействие от всички служители на Дружеството при изпълнение на служебните им задължения.

2. the right to request assistance from all employees of the Company in the performance of their official duties.

Длъжностно лице по защита на личните данни (ДЛЗЛД)

Data Protection Officer (DPO)

Чл. 30. (1) Съгласно изискванията на ОРЗД, Дружеството назначава ДЛЗЛД.

Art. 30. (1) According to the requirements of the GDPR, the Company appoints a DPO.

(2) ДЛЗЛД има следните задължения:

(2) The DPO has the following obligations:

1. информира и съветва Дружеството и неговите служителите законовите им задължения;

1. informs and advises the Company and its employees their legal obligations;

2. съблюдава спазването на законодателството за защитата на данни на равнище ЕС и на политиките на Дружеството по отношение на защитата на личните данни, включително възлагането на отговорности, повишаването на осведомеността и обучението на служителите, участващи в операциите по обработване, и съответните одити;

2. observes the observance of the data protection legislation at EU level and of the Company's policies regarding the protection of personal data, including the assignment of responsibilities, the raising of awareness and training of the employees involved in the processing operations and the respective audits;

3. предоставя съвети по отношение на оценката на въздействието върху защитата на данните;

3. provide advice regarding the assessment of the impact on data protection;

4. да отговаря на постъпили запитвания на субекти на данни във връзка с упражняването на правата им съгласно ОРЗД и настоящите правила;

4. to respond to received inquiries of data subjects in connection with the exercise of their rights according to the GDPR and these Rules;

5. сътрудничи с надзорния орган.

5. cooperate with the supervisory body.

Чл. 31. При изпълнението на своите задължения ДЛЗЛД надлежно отчита рисковете, свързани с операциите по обработване, и се съобразява с естеството, обхвата, контекста и целите на обработката. ДЛЗЛД е лицето за контакт между Дружеството и надзорния орган по всички въпроси, свързани с обработването и защитата на лични данни.

Art. 31. In carrying out its duties, the DPO shall take due account of the risks associated with processing operations and shall take into account the nature, scope, context and objectives of the processing. DPO is the contact person between the Company and the supervisory authority on all matters related to the processing and protection of personal data.

Чл. 32. (1) В случай на нарушение на сигурността на личните данни ДЛЗЛД, без ненужно забавяне и когато това е осъществимо — не по-късно от 72 часа след като е разбрал за него, уведомява за нарушението на сигурността на личните данни компетентния надзорен орган. Уведомлението до надзорния орган съдържа причините за забавянето, когато не е подадено в срок от 72 часа.

Art. 32. (1) In case of violation of the security of the personal data DPO, without unnecessary delay and when this is feasible - not later than 72 hours after having found out about it, shall notify about the violation of the security of the personal data to the competent supervisory body. The notification to the supervisory authority shall contain the reasons for the delay when it is not submitted within 72 hours.

(2) Образец на уведомление от Дружеството до надзорния орган в случай на нарушение на сигурността на личните данни се съдържа в Приложение № 3.

(2) A sample notification from the Company to the supervisory body in case of breach of personal data security is contained in Schedule 3.

Отдел „Информационни технологии“

Information Technology Department

Чл. 32а. (1) (Нов - 04.04.2025 г.) Отдел „Информационни технологии” осигурява информационното и техническото обслужване на

Art. 32a (1) (New - 4th of April 2025) The Information Technology Department provides the information and technical services of the Company regarding the

Дружеството по отношение на обработването и защитата на лични данни, включително на отделите и длъжностите, отговорни за тези дейности.

(2) Във връзка със законосъобразното обработване и защита на лични данни отдел „Информационни технологии" има следните задължения:

1. информира, съветва и съдейства на Дружеството и неговите служители относно предприемането на съответните необходими технически и организационни мерки;

2. определя, съблюдава и поддържа правилното функциониране на използваните от Дружеството информационни системи и/или мрежи;

3. осъществява редовна профилактика на компютрите и комуникационните средства;

4. осигурява, съблюдава и поддържа физическата защита (определяне на зоните с контролиран достъп и на използваните технически средства за физическа защита) в Дружеството;

5. организира и осигурява персонална защита съобразно предвиденото в настоящите правила;

6. осигурява псевдонимизация и криптографска защита;

7. предприема всички други действия и мерки, необходими за обезпечаване на законосъобразното обработване и защита на лични данни съгласно настоящите правила.

processing and protection of personal data, including the departments and positions responsible for these activities.

(2) In connection with the lawful processing and protection of personal data the Information Technology Department has the following obligations:

1. informs, advises and assists the Company and its employees regarding the taking of the necessary technical and organisational measures;

2. defines, supervises and maintains the automated information systems and/or networks;

2. undertakes regular maintenance of computers and communications;

4. ensures, supervises and maintains the physical protection (determination of the zones with controlled access and of the used technical means for physical protection) in the Company:

5. organises and ensures the personal protection in compliance with these Rules;

6. ensures the pseudonymisation and cryptographic protection;

7. undertakes any other actions and measures necessary to ensure the lawful processing and protection of personal data in accordance with these Rules.

ГЛАВА V. ТЕХНИЧЕСКИ И ОРГАНИЗАЦИОННИ МЕРКИ ЗА ОСИГУРЯВАНЕ НА НЕОБХОДИМОТО НИВО НА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

Чл. 33. Личните данни от Регистър „Клиенти", Регистър „Служители", Регистър „Контрагенти" и Регистър „Доставчици" (ако е приложимо) се въвеждат в базата данни на Дружеството, които са свързани в локална мрежа, със защитен достъп.

CHAPTER V. TECHNICAL AND ORGANIZATIONAL MEASURES FOR ENSURING THE NECESSARY LEVEL OF PROTECTION AND PROTECTION

Art. 33. The personal data from the Clients' Register, the Employees' Register, the Contractors' Register and the Suppliers' Register (if applicable) shall be entered in the database of the Company, which are connected in a local network, with secure access.

Чл. 34. В Дружеството са определени различни нива на достъп до лични данни, съхранявани на електронен носител, в зависимост от длъжностната характеристика на всеки служител на Дружеството и естеството на неговите служебни задължения.

Art. 34. The Company has defined different levels of access to personal data stored on electronic media, depending on the job description of each employee of the Company and the nature of his official duties.

Чл. 35. (Изм. 04.04.2025 г.) След направен подробен анализ на обработването на лични данни и оценката на въздействието върху защитата на лични данни, Дружеството определя ниско ниво на въздействие за всички поддържани регистри и ниско ниво на защита на личните данни, обработвани в Дружеството, съгласно критериите, определени в ОРЗД и Закона за защита на личните данни.

Art. 35. (Amended on the 4th of April 2025) After a detailed analysis of the processing of personal data and the assessment of the impact on personal data protection, the Company determines a low level of impact for all maintained registers and a low level of protection of personal data processed in the Company, according to the criteria set out in the GDPR and the PDPA.

Дружеството оценява нивото на въздействие за всеки поддържан регистър, както следва:

The Company assesses the level of impact for each maintained register as follows:

	Ниво на въздействие / Level of impact	Поверителност / Confidentiality	Цялостност / Integrity	Наличност / Availability	Общо за регистъра / Total for the register
Регистър „Клиенти” / Clients’ Register	Ниско / Low	Ниско / Low	Ниско / Low	Ниско / Low	Ниско / Low
Регистър „Служители” / Employees’ Register	Ниско / Low	Ниско / Low	Ниско / Low	Ниско / Low	Ниско / Low
Регистър „Контрагенти‘‘ / Contractors’ Register	Ниско / Low	Ниско / Low	Ниско / Low	Ниско / Low	Ниско / Low
Регистър „Доставчици” / Suppliers’ Register	Ниско / Low	Ниско / Low	Ниско / Low	Ниско / Low	Ниско / Low

Чл. 36. Съгласно настоящите правила, видовете защита и нейните нива са следните:

Art. 36. According to these Rules, the types of protection and its levels are the following:

1. автоматизирани информационни системи и/или мрежи, включващи следното:

а) непосредствен достъп до локалната мрежа имат само определени служители на Дружеството чрез комбинацията от служебно предоставено устройство и персонален акаунт. Служителите имат достъп само до данни и ресурси, необходими за изпълнение на служебните им задължения. Към използваните пароли е налице изискване за определена сложност. За да бъдат валидни те трябва да съдържат минимум шест символа, да бъдат съчетание от малки и големи букви, цифри и специални знаци. Паролите се сменят задължително на всеки шестдесет дни. При погрешно въвеждане на дадена парола повече от три пъти, потребителят се заключва автоматично и не може да използва мрежовите ресурси без намеса на системния администратор;

б) за осигуряване надеждност и интегритет на компютърната система, Дружеството прилага различни практики, включително, но не само, сигурна конфигурация на устройствата, редовни външни и вътрешни проверки за уязвимости, регулярно обновяване, филтриране на входящия и изходящия трафик, резервно захранване, отделяне на сървъри в специално помещение, разделяне на мрежата на сегменти за осигуряване на по-висока сигурност, периодични копия и други.

2. осъществяване на редовна профилактика на компютрите и комуникационните средства, включващо:

а) профилактика на компютрите и проверка за вируси, шпионски и рекламен софтуер, проверка на твърди дискове за грешки, дефрагментация на твърди дискове, актуализация на операционната система и използвания софтуер;

б) за предпазване на компютърната мрежа от неправомерен достъп през интернет се използва специализирано устройство – защитна стена (Firewall), което следи и филтрира входящия и изходящия трафик, премахвайки автоматично зловреден код и

1. automated information systems and/or networks, including the following:

a) only certain employees of the Company have direct access to the local network through the combination of officially provided device and personal account. Employees have access only to data and resources necessary for the performance of their official duties. The passwords used require a certain complexity. To be valid, they must contain a minimum of six characters, be a combination of lowercase and uppercase letters, numbers and special characters. Passwords must be changed every sixty days. If a password is entered incorrectly more than three times, the user is locked automatically and cannot use the network resources without the intervention of a system administrator;

b) to ensure the reliability and integrity of the computer system, the Company applies various practices including, but not limited to, secure device configuration, regular external and internal vulnerability checks, regular updates, filtering of incoming and outgoing traffic, backup power, server separation in a special room, dividing the network into segments to ensure higher security, periodic copies and others.

2. regular maintenance of computers and communications, including:

a) computer maintenance and virus, spyware and adware scanning, hard disk checks for errors, hard disk defragmentation, operating system updates and software used;

b) to protect the computer network from unauthorised access via the Internet, a specialised device is used - a firewall, which monitors and filters incoming and outgoing traffic, automatically removing malicious code and blocking all connections except those explicitly allowed;

блокирайки всички връзки, освен изрично разрешените;

в) профилактика на компютрите и комуникационните средства, която се извършва от системните администратори ежедневно, на място в офиса на Дружеството и чрез отдалечен достъп, когато е необходимо;

г) при идентифициране на инциденти, за резултата от проверката се уведомяват лицата, представляващи Дружеството.

3. физическа защита (определяне на зоните с контролиран достъп и на използваните технически средства за физическа защита):

а) офисът на Дружеството, в който са поставени компютрите, се заключва и се достъпва от съответните служители, които работят в съответното помещение и разполагат с копие от ключа. Етажите, на които има компютри, които поддържат офисната мрежа на Дружеството, са снабдени със сигнално-охранителна система с цел осигуряване по-висока степен на защита на съхраняваните данни;

б) всички входове и изходи, включително стълбищата, се намират под постоянно видеонаблюдение. Записите се пазят централизирано съгласно изискванията на Закона за частната охранителна дейност и са достъпни само за оторизираните лица;

в) Дружеството не съхранява лични данни на сървъри, разположени в офисните помещения. Сървърите на Дружеството, на които се съхранява информация, включително информация, която представлява търговска тайна и лични данни, са разположени в сертифицирани по стандартите за сигурност ISO2700x дата центрове. Достъпът до тях на логическо ниво се осъществява чрез криптирана отдалечена връзка по специално наети частни канали, а на физическо ниво само от определени служители, с предварително записване на час и след одобрение от отговорника за съответния дата център от Дружеството и удостоверяването на самоличността от охраната.

c) prevention of computers and communication facilities, which is performed by system administrators on a daily basis, on site at the Company's office and through remote access, when necessary;

d) in case of identification of incidents, the persons representing the Company shall be notified of the result of the inspection.

3. physical protection (determination of the zones with controlled access and of the used technical means for physical protection):

a) the office of the Company, in which the computers are placed, is locked and accessed by the respective employees who are working there and has a copy of the key. The floors on which there are computers that support the office network of the Company are equipped with an alarm and security system in order to ensure a higher degree of protection of the stored data;

b) all entrances and exits, including staircases, shall be under continuous video surveillance. The records are kept centrally in accordance with the requirements of the Private Security Activity Act and are accessible only to authorised persons;

c) The company does not store personal data on servers located in the office premises. The Company's servers, on which information is stored, including information that is a trade secret and personal data, are located in ISO2700x certified data centres. Access to them at the logical level is through an encrypted remote connection through specially hired private channels, and at the physical level only by certain employees, with prior appointment and after approval by the responsible person for the relevant date centre of the Company and security authentication.

4. персонална защита:

а) офисът на Дружеството е в пълно съответствие с нормативните изисквания за пожарна безопасност и е снаден със специални средства за защита от пожар. Ръководителят на всеки отдел следи за спазването на мерките за безопасност в съответното помещение;

б) всеки служител е длъжен да споделя констатирана от него критична информация. Всеки служител, отговорен за обработването на лични данни и/или имащ достъп до тях, е длъжен да познава и прилага правилата за защита на личните данни.

5. документална защита:

а) непосредствен достъп до данните на хартиен носител от регистър „Служители" имат само определени служители, включително отдел „Счетоводство", който извършва превод на работните заплати, както и управителите на Дружеството.

б) достъп до Регистър „Доставчици" и Регистър „Контрагенти'' имат служителите, на които данните от съответния регистър са необходими за изпълнение на служебните им задължения, а именно: служителите от отдел „Нормативно съответствие", отдел „Счетоводство", управителите на Дружеството. Личните данни, съхранявани на хартиен носител, са разположени в обособени помещения и заключващи се шкафове, достъп до който имат само оторизираните за това служители.

6. псевдонимизация и криптографска защита:

а) Дружеството въвежда, както към момента на определянето на средствата за обработване, така и към момента на самото обработване, подходящи технически и организационни мерки, които са разработени с оглед на ефективното прилагане на принципите за защита на данните, които включват, inter alia, псевдонимизация, свеждане на данните до минимум, както и интегриране на необходимите гаранции в процеса на обработване, за да се спазят

4. personal protection:

a) the office of the Company is in full compliance with the normative requirements for fire safety and is equipped with special means for fire protection. The head of each department monitors the observance of the safety measures in the respective room;

b) each employee is obliged to share critical information found by him. Every employee responsible for the processing of personal data and/or having access to them is obliged to know and apply the rules for personal data protection.

5. documentary protection:

a) only certain employees, including the Accounting Department, who transfer salaries, as well as the Directors, have direct access to the data on paper from the Employees Register of the Company.

b) access to the Suppliers' Register and the Contractors' Register shall be granted to the employees whose data from the respective register are necessary for the performance of their official duties, namely: the employees from the Regulatory Compliance Department, the Accounting Department, the Directors of the Company. Personal data stored on paper are located in separate rooms and lockable cabinets, to which only authorised employees have access.

6. pseudonymization and cryptographic protection:

a) The Company introduces, both at the time of determining the means of processing and at the time of processing, appropriate technical and organisational measures that have been developed in order to effectively apply the principles of data protection, which include, inter alia, pseudonymisation, minimization of data, as well as integration of the necessary safeguards in the processing process in order to comply with the requirements of the DPA and to ensure the protection of the rights of data subjects;

изискванията на ОРЗД и да се осигури защита на правата на субектите на данни;

б) Дружеството въвежда псевдонимизация на личните данни на етап проектиране и по подразбиране. Дружеството счита, че прилагането на псевдонимизация на личните данни може да намали съществено рисковете за съответните субекти на данни и да помогне на Дружеството да изпълнява своите задължения за защита на данните;

b) the Company introduces pseudonymization of personal data at the design stage and by default. The Company considers that the application of pseudonymisation of personal data can significantly reduce the risks for the respective data subjects and help the Company to fulfil its data protection obligations;

в) в допълнение, Дружеството използва криптографските възможности на операционните системи за управление на бази данни и стандартните криптографски възможности на комуникационното оборудване. Конкретните протоколи и системи, разрешени за използване, са описани в „Стандарт за информационна сигурност“ и се обновяват регулярно.

c) in addition, the Company uses the cryptographic capabilities of the database management operating systems and the standard cryptographic capabilities of the communication equipment. The specific protocols and systems authorized for use are described in the Information Security Standard and are updated regularly.

ГЛАВА VI. ДЕЙСТВИЯ ЗА ЗАЩИТА ПРИ АВАРИИ, ПРОИЗШЕСТВИЯ И БЕДСТВИЯ

CHAPTER VI ACTIONS FOR PROTECTION IN ACCIDENTS, ACCIDENTS AND DISASTERS

чл. 37. (1) Всеки служител на Дружеството е длъжен да уведоми незабавно ДЛЗЛД при възникване на авария, произшествие и бедствие, при който е или би могла да бъде засегната сигурността на съхраняваните лични данни в базата данни на Дружеството.

Art. 37. (1) Each employee of the Company shall be obliged to notify immediately the DPO in case of an accident, accident and disaster, in which the security of the stored personal data in the database of the Company is or could be affected.

(2) Непосредствено след като е уведомено за настъпването на инцидент по ДЛЗЛД и/или служител от отдел „Нормативно съответствие‘‘ следва да предприеме всички необходими действия за потвърждаване на валидността на уведомлението, ограничаване на щетите и бъдещо предотвратяване, в т.ч. да уведоми лицата, представляващи Дружеството.

(2) Immediately after being notified of the occurrence of an incident under the DPO and/or an employee of the Regulatory Compliance Department shall take all necessary actions to confirm the validity of the notification, limit the damage and future prevention, incl. to notify the persons representing the Company.

(3) При първа възможност ДЛЗЛД уведомява представляващите Дружеството лица за събитието по ал. 1, като ги информира за:

(3) As soon as possible, the DPO shall notify the persons representing the Company of the event under para 1, informing them of:

1. описание на инцидента;

1. description of the incident;

2. времето на установяването на инцидента;

2. the time of the establishment of the incident;

3. лицето, което докладва за инцидента;

4. последствията от инцидента и мерките за отстраняването му.

(4) В случай на нарушение на сигурността на личните данни ДЛЗЛД, без ненужно забавяне и когато това е осъществимо — не по-късно от 72 часа след като е го е потвърдил, уведомява за нарушението на сигурността на личните данни компетентния надзорен орган, а именно Комисията по защита на личните данни. Уведомлението до надзорния орган съдържа причините за забавянето, когато не е подадено в срок от 72 часа.

(5) В уведомлението до компетентния надзорен орган съгласно предходния член се съдържа най-малко следното:

1. описание на естеството на нарушението на сигурността на личните данни, включително, ако е възможно, категориите и приблизителният брой на засегнатите субекти на данни и категориите и приблизителното количество на засегнатите записи на лични данни;

2. посочване на името и координатите за връзка на ДЛЗЛД, от което може да се получи повече информация;

3. описание на евентуалните последици от нарушението на сигурността на личните данни;

4. описание на предприетите от Дружеството мерки за справяне с нарушението на сигурността на личните данни, включително мерките за намаляване на евентуалните неблагоприятни последици.

(6) Образец на уведомление до надзорния орган в случай на нарушение на сигурността на личните данни се съдържа в Приложение № 4.

(7) Дружеството документира всяко реално нарушение на сигурността на личните данни, включително фактите, свързани с нарушението на

3. the person who reports the incident;

4. the consequences of the incident and the measures for its elimination.

(4) In case of violation of the security of personal data, the DPO, without undue delay and when this is feasible - not later than 72 hours after having confirmed it, shall notify the competent supervisory body of the violation of the security of personal data, and namely the Commission for Personal Data Protection. The notification to the supervisory authority shall contain the reasons for the delay when it is not submitted within 72 hours.

(5) The notification to the competent supervisory authority according to the previous article shall contain at least the following:

1. description of the nature of the personal data breach, including, if possible, the categories and the approximate number of data subjects and categories and the approximate amount of personal data records concerned;

2. indication of the name and contact details of the DPO, from which more information can be obtained;

3. description of the possible consequences of the violation of the security of the personal data;

4. description of the measures taken by the Company to address the breach of personal data security, including measures to reduce any adverse effects.

(6) A sample notification to the supervisory body in case of personal data breach is contained in Schedule 4.

(7) The company shall document any actual breach of personal data security, including the facts related to the personal data breach, its consequences and the actions taken to deal with it.

сигурността на личните данни, последиците от него и предприетите действия за справяне с него.

ГЛАВА VII. СЪОБЩАВАНЕ НА СУБЕКТА НА ДАННИТЕ ЗА НАРУШЕНИЕ НА СИГУРНОСТТА НА ЛИЧНИТЕ ДАННИ

Чл. 38. (1) Когато има вероятност нарушението на сигурността на личните данни да породи висок риск за правата и свободите на физическите лица, Дружеството, без ненужно забавяне, съобщава на субекта на данните за нарушението на сигурността на личните данни.

(2) В съобщението до субекта на данните, на ясен и точен език се описва естеството на нарушението на сигурността на личните данни и се посочват най-малко информацията, която е съобщена от ДЛЗЛД на компетентния надзорен орган.

(3) Съобщение до субекта на данните не се изисква, ако някое от следните условия е изпълнено:

1. Дружеството е предприело подходящи технически и организационни мерки за защита и тези мерки са били приложени по отношение на личните данни, засегнати от нарушението на сигурността на личните данни, по-специално мерките, които правят личните данни неразбираеми за всяко лице, което няма разрешение за достъп до тях, като например криптиране;

2. Дружеството е взело мерки, които гарантират, че вече няма вероятност да се материализира високият риск за правата и свободите на субектите на данни;

3. подобно съобщение би довело до непропорционални усилия. В такъв случай се прави публично съобщение или се взема друга подобна мярка, така че субектите на данни да бъдат в еднаква степен ефективно информирани.

CHAPTER VII. COMMUNICATION OF THE DATA SUBJECT FOR VIOLATION OF THE SECURITY OF PERSONAL DATA

Art. 38. (1) When there is a probability that the violation of the security of the personal data will cause a high risk for the rights and freedoms of the natural persons, the Company, without unnecessary delay, shall inform the data subject about the violation of the security of the personal data.

(2) The communication to the data subject shall, in clear and precise language, describe the nature of the personal data breach and shall indicate at least the information communicated by the DPO to the competent supervisory authority.

(3) Communication to the data subject is not required if any of the following conditions is met:

1. the company has taken appropriate technical and organisational protection measures and these measures have been applied to personal data affected by the breach of security. personal data, in particular measures that make personal data incomprehensible to any person who does not have permission to access it, such as encryption;

2. the Company has taken measures to ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise;

3. such a communication would lead to disproportionate efforts. In such a case, a public announcement shall be made or another similar measure shall be taken so that the data subjects are equally effectively informed.

ГЛАВА VIII. СЪХРАНЯВАНЕ, АРХИВИРАНЕ И УНИЩОЖАВАНЕ НА ЛИЧНИ ДАННИ

Чл. 39. Личните данни се съхраняват на сървъри в мрежата на Дружеството. Системните

CHAPTER VIII. STORAGE, ARCHIVING AND DESTRUCTION OF PERSONAL DATA

Art. 39. Personal data is stored on servers in the network of the Company. System administrators regularly back up

администратори архивират регулярно данните от сървърите във всеки дата център на дискови масиви в другия дата център.

the data from the servers in each data centre to disk arrays in the other data centre.

чл. 40. Прехвърлянето на данни от регистрите на друг администратор може да бъде извършвано само след предварително уведомяване на Комисията, ако прехвърлянето е предвидено в закон и е налице идентичност на целите на обработването.

Art. 40. The transfer of data from the registers to another controller may be carried out only after prior notification to the Commission, if the transfer is provided by law and there is an identity of the purposes of the processing.

Чл. 41. Създават се временни файлове за необходимото техническо време за импорт на данни. Файловете се унищожават автоматично до една минута след приключване на импорта. Временните файлове се съхраняват в защитена папка с данни на сървъра, до която имат достъп само определени служители.

Art. 41. Temporary files are created for the necessary technical time for data import. The files are automatically destroyed within one minute after the import is completed. Temporary files are stored in a secure data folder on the server, which is accessible only to certain employees.

Чл. 42. Дружеството съхранява личните данни в Регистър „Клиенти‘‘ в продължение на целия период на съществуване на договорните отношения със съответния клиент, но не по-малко от 5 години след прекратяване на договорните отношения с него, независимо от причините за прекратяването.

Art. 42. The Company shall store the personal data in the Clients' Register for the entire period of existence of the contractual relations with the respective client, but not less than 5 years after the termination of the contractual relations with him, regardless of the reasons for termination.

Чл. 43. Дружеството съхранява личните данните в Регистър „Контрагенти‘‘ в продължение на целия период на съществуване на договорните отношения със съответния контрагент, но не по-малко от 5 години след прекратяване на договорните отношения с контрагента, независимо от причините за прекратяването.

Art. 43. The Company shall keep the personal data in the Contractors' Register for the entire period of existence of the contractual relationship with the respective contractor, but not less than 5 years after the termination of the contractual relationship with the contractor, regardless of the reasons for termination.

Чл. 44. (1) Дружеството съхранява следните лични данни от Регистър „Служители“ за срок не по-дълъг от 50 (петдесет) години от възникването на трудовото правоотношение: трудов договор, длъжностна характеристика, ведомости за заплати. Отделни лични данни от Регистър „Служители“ се съхраняват за по-кратък срок, като например болнични листове, които се съхраняват за срок от 3 (три) години, считано от началната дата на издаване на болничния лист. Личните данни по настоящия член се съхраняват на хартиен и електронен носител.

Art. 44. (1) The Company shall store the following personal data from the Employees' Register for a period not longer than 50 (fifty) years from the occurrence of the employment relationship: employment contract, job description, payroll. Individual personal data from the Employees' Register are stored for a shorter period, such as sick leaves, which are stored for a period of 3 (three) years from the starting date of issuance of the sick leave. Personal data under this Article shall be stored on paper and electronic media.

(2) Подробно описание на всички приложими срокове за съхранение на лични данни от Регистър „Служители‘‘ се съдържат в Приложение „Срокове за съхранение на документи“ към Вътрешна процедура за работа с лични данни в отдел „Счетоводство“.

(2) Detailed description of all applicable terms for storage of personal data from the Employees' Register are contained in Schedule - Terms for Storage of Documents to the Internal procedure for work with personal data in the Accounting Department.

(3) Отдел „Нормативно съответствие“ отговаря за правилното съхраняване на личните данни в съответните регистри. Унищожаването на лични данни може да бъде извършвано само от определени служители след изрична инструкция на отдел „Нормативно съответствие”, в която са указани видовете лични данни, срокът и начинът на унищожаване.

(3) The Regulatory Compliance Department shall be responsible for the proper storage of personal data in the respective registers. The destruction of personal data may be carried out only by certain employees after an explicit instruction of the Regulatory Compliance Department, which indicates the types of personal data, the term and manner of destruction.

Чл. 45. В допълнение, след изтичане на гореспоменатите срокове за съхранение, отдел „Нормативно съответствие” издава инструкция за унищожаването на съответните лични данни, чрез която възлага на определен служител тяхното унищожаване, както следва:

Art. 45. In addition, after the expiration of the above-mentioned storage terms, the Regulatory Compliance Department shall issue an instruction for the destruction of the respective personal data, by which it shall assign to a certain employee their destruction, as follows:

1. лични данни, съхранявани на хартиен носител – машинно унищожаване чрез шредер;

1. personal data stored on paper - machine shredder destruction;

2. лични данни, съхранявани на електронен носител – изтриване от електронната база данни/ сървъри.

2. personal data stored on electronic media - deletion from the electronic database / servers.

ГЛАВА IX. ПРЕДОСТАВЯНЕ НА ЛИЧНИ ДАННИ НА ТРЕТИ ЛИЦА И УПРАЖНЯВАНЕ ПРАВАТА НА СУБЕКТИТЕ НА ЛИЧНИ ДАННИ

CHAPTER IX. PROVISION OF PERSONAL DATA TO THIRD PARTIES AND EXERCISE OF THE RIGHTS OF THE SUBJECTS OF PERSONAL DATA

Чл. 46. Дружеството има право да разкрива информация относно съхраняваните лични данни само:

Art. 46. The Company has the right to disclose information about the stored personal data only:

1. на субекта на данни или на изрично упълномощено от него лице, което предоставя нотариално заверено пълномощно с представителна власт, при спазване на процедурите за достъп до личните данни;

1. to the data subject or to a person explicitly authorised by him, who provides a notarized power of attorney with representative authority, in compliance with the procedures for access to personal data;

2. на свои контрагенти, когато обработването е необходимо за изпълнението на договор между Дружеството и контрагента, при спазване на законодателството за защита на личните данни;

2. to its contractors, when the processing is necessary for the performance of a contract between the Company and the contractor, in compliance with the legislation for protection of personal data;

3. на оправомощените държавни органи в определените от закона случаи и по определения от закона ред.

3. to the authorised state bodies in the cases determined by the law and by the order determined by the law.

ГЛАВА X. ОБУЧЕНИЕ НА СЛУЖИТЕЛИТЕ

CHAPTER X. TRAINING OF EMPLOYEES

Чл. 47. (1) При постъпване на работа в Дружеството, ДЛЗЛД запознава всеки служител с настоящите правила и нормативните документи, свързани с мерките за защита на личните данни, което се удостоверява с подписването на декларация.

Art. 47. (1) Upon entering work in the Company, the DPO shall acquaint each employee with these Rules and the normative documents, related to the measures for protection of the personal data, which shall be certified by signing a declaration.

(2) ДЛЗЛД периодично информира служителите на Дружеството за настъпили промени в начина на защита на личните данни, включително за промени в настоящите правила и/или за промени в нормативната уредба. За всеки проведен инструктаж по предходното изречение се изготвя и подписва протокол.

(2) The DPO periodically informs the employees of the Company about changes in the manner of personal data protection, including changes in these Rules and/or changes in the regulations. A protocol shall be prepared and signed for each conducted instruction under the previous sentence.

(3) Всеки служител на Дружеството преминава индивидуално обучение, което обучение го запознава с изискванията на ОРЗД. Всички новопостъпили служители на работа в Дружеството преминават същото обучение в срок от 3 (три) работни дни след постъпването им на работа.

(3) Each employee of the Company passes an individual training, which acquaints him/her with the requirements of GDPR. All newly hired employees of the Company undergo the same training within 3 (three) working days after starting work.

ГЛАВА XI. ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

CHAPTER XI. FINAL PROVISIONS

§ 1. (1) (Изм. 04.04.2025 г.) Настоящите правила се приемат на основание ОРЗД, ЗЗЛД и останалите подзаконови нормативни актове на Република България.

§ 1. (1) (Amended on the 4th of April 2025). These Rules are adopted on the basis of the GDPR, PDPA and the other by-laws of the Republic of Bulgaria.

(2) Настоящите правила са приети в двуезична версия - на български и английски език. При противоречие между двете езикови версии българската версия ще има предимство.

(2) These Rules have been adopted in bilingual versions - in Bulgarian and English language. In case of contradiction between the two language versions - the Bulgarian language version shall prevail.

§ 2. Изброените по - долу процедури и образци представляват неразделна част от настоящите правила:

§ 2. The following procedures and samples are an integral part of these Rules:

1. Приложение № 1 – Процедура за работа при постъпили молби от клиенти на Дружеството във

1. Schedule 1 - Procedure for work on requests from clients of the Company in connection with the exercise of their rights under the Regulation;

връзка с упражняване на правата им съгласно Регламента;

2. Приложение № 2 – Процедура за работа при постъпили молби от служители на Дружеството във връзка с упражняване на правата им съгласно ОРЗД;

3. Приложение № 3 – Образец на уведомление до надзорния орган в случай на нарушение на сигурността на личните данни.

§ 3. (Изм. 04.04.2025 г.) Настоящите правила са приети на 15.02.2025 г. и са съответно изменени на 04.04.2025 г. от управителя на Дружеството.

2. Schedule 2 - Procedure for work in case of received requests from employees of the Company in connection with the exercise of their rights under the ORD;

3. Schedule 3 - Model notification to the supervisory authority in case of breach of personal data security.

§ 3. (Amended on the 4th of April 2025) These Rules have been adopted on the 15th of February 2025 and have been subsequently amended on the 4th of April 2025 by the Director of the Company.