SEEBURGER
BUSINESS INTEGRATION

GDPR
Seeburger Informatik EOOD

ВЕРСИЯ 0.1

иновативност признателност доверие устойчивост работа в екип

SEEBURGER
BUSINESS INTEGRATION

ПОЛИТИКА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

PRIVACY POLICY

1. Въведение

Настоящата Политика за защита на личните данни на субекти на данни („Политика за поверителност“) описва как **„Зеебургер - информатик“ ЕООД (“Компанията“, „Администратор“)** и/или свързаните с него дружества третират личните данни на нашите клиенти, доставчици, служители, кандидати за работа, трети страни и други лица, намиращи се в рамките на ЕС, или чиито Лични данни попадат под обхвата на европейското законодателство за защита на личните данни по други причини.

Определенията на термините, изписани с главни букви, са посочени в Приложение А към настоящата Политика за поверителност.

Настоящата Политика за поверителност се прилага по отношение на всички Лични данни, които обработваме, независимо от носителя, върху който се съхраняват данните и независимо дали се отнасят до бивши или настоящи служители, кандидати за работа, контрагенти, трети страни или други Субекти на данни.

1. Introduction

This Policy (the `Privacy Policy`) explains how **Seeburger Informatik EOOD hereinafter referred to as `the Company` / `the Controller`** and /or its affiliates handle the Personal data relating to our customers, suppliers, employees, job applicants, third parties and other persons located within the EU or whose personal data fall within the scope of European Data Protection Legislation for other reasons. Definitions of capitalized terms are set out in Appendix A to this Privacy Policy.

The present Privacy Policy applies to the use of any and all Personal Data processed by us, regardless of a data storage medium and whether the data relate to former or current employees, job applicants, contractors, third parties or other Data Subjects.

2. Обхват

Убедени сме, че правилното и законно третиране на Личните данни поддържа доверието в организацията и осигурява основата за успешна бизнес дейност. Защитата на поверителността и целостта на Личните данни представлява важна отговорност, която възприемаме изключително сериозно, във всеки един момент.

Правилата на Общия регламент за защита на личните данни („ОРЗД“) важат за всички администратори на лични данни, които са

2. Scope

We are convinced that the correct and legal treatment of Personal Data maintains the trust in the Company and provides the basis for successful business activity. Protecting the confidentiality and integrity of Personal Data is an important responsibility that we take very seriously at all times.

The rules of EU General Data Protection Regulation, hereinafter referred to as `the GDPR`, apply to all Personal data controllers estab-

установени в ЕС и обработват лични данни на физически лица, в контекста на своята дейност. „Зеебургер - информатик“ ЕООД е Администратор на лични данни по смисъла на чл. 4, т. 7 от ОРЗД.

lished in the EU which process Personal data of individuals as part of its activity. Seeburger Informatik EOOD is a Personal Data Controller within the meaning of Art. 4, item 7 of GDPR.

Ръководството на „Зеебургер - информатик“ ЕООД се ангажира да осигури съответствие с българското и европейското законодателство по отношение на обработването на личните данни и защитата на правата и свободите на лицата, чиито лични данни Компанията събира и обработва съгласно Общия регламент за защита на данните.

The management of Seeburger Informatik EOOD undertakes to ensure compliance with the Bulgarian and European legislation regarding the processing of Personal data and the protection of the rights and freedoms of the individuals whose personal data the Company collects and processes in accordance with the General Data Protection Regulation.

Общият регламент за защита на личните данни и настоящата Политика се отнасят до всички функции по обработването на Лични данни, включително тези, които се извършват относно клиенти, служители, доставчици и партньори и всякакви други лични данни, които Компанията обработва от различни източници.

The General Data Protection Regulation and this Policy apply to all personal data processing functions, including those performed concerning customers, employees, suppliers and partners, as well as to any other Personal data that the Company processes from various sources.

Длъжностното лице по защита на данните отговаря за преразглеждането на дейностите по обработване ежегодно в светлината на всякакви промени в дейностите на Компанията, както и всички допълнителни изисквания и оценки на въздействието върху защитата на данните.

The Data Protection Officer is responsible for reviewing the processing activities annually in the light of any changes in the Company’s activities, as well as any additional requirements and data protection impact assessments.

Тази Политика се прилага за всички служители и външни контрагенти и доставчици на Компанията. Всяко нарушение на Общия регламент ще бъде разглеждано като нарушение на трудовата дисциплина, а в случай че има предположение за извършено престъпление, въпросът ще се предостави за разглеждане в най-кратък срок на съответните държавни органи.

This Policy applies to all employees and external contractors and suppliers of the Company. Any breach of the GDPR will be considered as a violation of labour discipline, and in case of a suspicion of a crime committed, the matter will be referred to the relevant state authorities as soon as possible.

Партньори и трети лица, които работят с или за „Зеебургер - информатик“ ЕООД, както и лица, които имат или могат да

Partners and third parties who work with or for Seeburger Informatik EOOD, as well as persons who have or may have access to Per-

имат достъп до личните данни, ще се очаква да се запознаят, разбират и да се съобразят с тази Политика.Никоя трета страна не може да има достъп до Лични данни, съхранявани от Компанията, без предварително да е сключила споразумение за поверителност на данните, което налага на третата страна задължения, не по-малко обременяващи от тези, които Компанията е поела и което й дава право да извършва проверки за спазването на наложените със споразумението задължения.

sonal data, will be expected to know, understand and comply with this Policy. No third party may have access to Personal data held by the Company without entering into a data confidentiality agreement, which imposes on the third party obligations no less burdensome than those undertaken by the Company and which gives us the right to carry out inspections for compliance with the obligations imposed by the agreement.

„Зеебургер - информатик" ЕООД предоставя изложена на ясен и лесноразбираем език подробна и конкретна информация на Субектите на данни, посредством подходящи Уведомления за поверителност в сбит, прозрачен, разбираем и лесно достъпен формат.

Seeburger Informatik EOOD provides detailed information to the Data Subjects in a clear, easy-tounderstand language, through appropriate Privacy Notices in a concise, understandable and transparent manner and easily accessible form.

Длъжностното лице по защита на данните отговаря за координирането и наблюдението на спазването на изискванията на Общия регламент и настоящата Политика за поверителност. Можете да се свържете с него на dpo.bg@seeburger.com и да отправяте всякакви въпроси относно прилагането на настоящата Политика за поверителност.

The Data Protection Officer is responsible for coordinating and monitoring compliance with the requirements of the GDPR and this Privacy Policy. You can contact the DPO at dpo.bg@seeburger.com and ask any questions regarding the application of this Privacy Policy.

3. Принципи за защита на личните данни

3. Principles of Personal Data Protection

При обработката на Личните данни спазваме следните принципи, които изискват Лични данни:

We observe the following key principles related to the processing of Data Subjects Personal Data:

(а) Да се обработват законосъобразно, добросъвестно и прозрачно (Законност, Справедливост и IWeUJR).

(a) to be processed lawfully, in good faith and in a transparent manner (Lawfulness, Fairness and Transparency),

(б) Да се събират единствено за конкретни, изрични и законосъобразни цели Ограничаване на целите).

(b) to be collected only for specified, explicit and legitimate purposes (Purpose limitation),

(в) Да бъдат адекватни, свързани с

(c) to be adequate, related to the purpose for

целта, за която са събрани и ограничени до необходимото, с оглед целите на Обработката (Свеждане на данните до минимум).

which they are collected and limited to what is necessary in relation to the purposes for which they are processed (Data minimisation),

(г) Да бъдат точни, и, когато е необходимо, актуализирани (Точност).

(d) to be accurate and, where necessary, kept up to date (Accuracy),

(д) Да не се съхраняват във формат, който позволява идентифицирането на Субектите на данни за по-дълъг период, отколкото е необходим за целите на Обработката (Ограничаване на съхранението).

(e) to be kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data are processed (Storage limitation),

(е) Да се обработват по начин, който гарантира тяхната сигурност чрез използване на подходящи технически и организационни мерки за защита срещу неупълномощена или незаконна Обработка, както и срещу непреднамерена загуба, унищожаване или увреждане (Сигурност, Цялостност и Поверителност).

(f) to be processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical ot organizational measures (Integrity, Confidentiality and Security),

(ж) Да не се прехвърлят в друга държава без въвеждането на подходящи мерки за защита (Ограничение на трансферите).

(g) not to be transferred to another country without the implementation of appropriate safety measures (Data transfers limitation),

(з) Да се предоставят на Субектите на данни, като Субектите на данни да имат възможността да упражняват определени права по отношение на Личните си данни (Права и искания на Субектите на данни).

(h) not to be transferred to another country without the implementation of appropriate safety measures (Data transfers limitation),

„Зеебургер - информатик“ ЕООД идентифицира основанието за обработване преди да започне да обработва лични данни. Носим отговорност за спазването на всички принципи за защита на данните, посочени по-горе и сме в състояние да демонстрираме това съответствие (Отчетност). Всички способи за събиране на данни се преглеждат веднъж годишно от вътрешен одит/външни експерти, за да се гарантира, че събраните данни продължават да бъдат адекватни, релевантни, не са прекомерни като при

Seeburger Informatik EOOD identifies the legal grounds for personal data processing before we begin processing the data. We are responsible for complying with all data protection principles set out above and we are able to demonstrate this compliance (Accountability). All data collection methods are subject to once-a-year review by internal audit / external experts to ensure that the data collected continue to be adequate, relevant, not excessive and, if necessary, a data protection impact assessment is carried out.

необходимост се извършва оценка на въздействието върху защитата на данните.

Обработване на Лични данни се извършва само ако е налице някое от посочените основания:

(а) Обработката е необходима за изпълнението на договор, сключен със Субекта на данни;

(б) Обработката е необходима във връзка със задълженията ни за спазване на законови изисквания;

(в) Обработката е необходима за постигане на наши легитимни интереси и цели, при условие, че тези цели не са в ущърб на интересите или фундаменталните права и свободи на Субектите на данни;

(г) Субектът на данни е предоставил своето Съгласие.

Чувствителни лични данни могат да се обработват единствено ако:

(а) Е налице някое от основанията, посочени по-горе; и

(б) Изпълнено е едно от специалните условия за Обработка на Чувствителни лични данни, част от които са изброени по-долу:
- Обработката се налага с цел упражняване на права или задължения на Компанията или Субекта на данни, произтичащи от трудовото законодателство;
- Обработката се налага с цел защита с цел защита на жизнените интереси на Субекта на данни;
- Обработката се отнася до Лични данни, които са оповестени публично от Субекта на данни;
- Субектът на данни е предосавил Изрично съгласие.

Personal Data processing is carried out only if any of the following legal grounds applies:

(a) The Processing is necessary for the performance of contract to which the Data Subject is party;

(b) The Processing is necessary for compliance with a legal obligation to which the controller is subject;

(c) The Processing is necessary for the purposes of our legitimate interests, except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject;

(d) The Data Subject has given consent to the processing of his / her personal data.

Sensitive Personal Data may be processed only if the following conditions are met:

(a) There is any of the legal grounds for processing set out above, and

(b) One of the specific conditions for the Sensitive Personal Data Processing, some of which are listed below, has been met:
- The processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the Company or of the Data Subject in the field of employment;
- The processing is necessary to protect the vital
interests of the Data Subject;
- The Processing relates to Personal Data which are made public by the Data Subject;
- The Data Subject has given an Explicit consent.

Обработката на Чувствителни лични данни се извършва от служителите само след получаване на предварителното писмено одобрение на Длъжностното лице по защита на данните, освен в случаите когато Компанията е задължена да обработва такива данни по силата на нормативен акт.

The Sensitive Personal Data Processing is carried out by the employees only after obtaining the prior written approval of the Data Protection Officer, except where the Company is bound to process such data by virtue of a Law.

Администраторът трябва да предостави на Субекта на данни следната информация:
• данни, които идентифицират администратора и данните за контакт на администратора;
• данни за контакт с Длъжностното лице по защита на данните;
• целите на обработването и правното основание за обработването;
• периода, за който ще се съхраняват личните данни или, ако това не е възможно, критериите, които се използват за определяне на този период;
• правата на Субекта на данни - да поиска достъп до данните, коригиране, изтриване (право „да бъдеш забравен“), ограничаване на обработването, да оттегли даденото съгласие за обработването, без да се засяга законосъобразността на обработването преди оттеглянето, право на възражение срещу обработването или срещу условията (или липсата на такива) във връзка с упражняването на тези права, както и право на жалба до надзорния орган;
• категориите лични данни;
• получателите или категориите получатели на лични данни;
• дали администраторът възнамерява да прехвърли личните данни към получател в трета страна и нивото на защита на данните;
• всякаква допълнителна информация, необходима да се гарантира добросъвестно прозрачно обработване.

The Controller shall provide the Data Subject with the following information:
• the identity and the contact details of the Controller;
• the contact details of the Data Protection Officer;
• the purposes of the processing for which the Personal Data are intended as well as the legal basis for the processing;
• the period for which the Personal Data will be stored, or if that is not possible, the criteria used to determine that period;
• the rights of the Data Subject - the right to request from the controller access to and rectification or erasure of Personal Data (`right to be forgotten`) or restriction of processing, the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal, the right to object to processing or to the conditions (or lack thereof) in connection with the exercise of these rights, as well as the right to lodge a complaint with a supervisory authority;
• the categories of Personal Data;
• the recipients or categories of recipients of the Personal Data;
• whether the controller intends to transfer Personal Data to recipient located in a third country and the existence of appropriate or suitable safeguards;
• any additional information necessary to ensure fair and transparent processing.

Личните данни се поддържат точни и актуални във всеки един момент, като Компанията е положила всички разумни усилия, за да е възможно незабавно (в рамките на възможните технически

Personal Data held are accurate and kept up-to- date and the Company has taken every reasonable step (within possible technical solutions) to ensure that Personal Data that are inaccurate, having regard to the purpos-

решения) изтриване или коригиране на неточни или неактуални Лични данни, в зависимост от целите, за които са били обработени.

es for which they are processed, are erased or rectified without delay.

Данните се преглеждат и актуализират при необходимост. Не се съхраняват данни, когато има вероятност да не са точни. Целият персонал е обучен в значението на събирането на точни данни и поддържането им.

The Personal Data are reviewed, and where necessary, updated. Data are not stored when they are likely to be inaccurate. All employees are trained in the importance of collecting and maintaining accurate data.

Задължение на Субекта на данните е да гарантира, че данните, които предава за обработване и съхраняване от Компанията са точни и актуални. От служителите, клиентите, контрагентите и доставчиците се изисква да уведомяват Компанията за всякакви промени в обстоятелствата, за да могат да се актуализират записите на лични данни. Отговорността на Компанията е да гарантира, че всяко уведомление относно промяната на обстоятелствата е записано и се предприемат съответни действия.

The Data Subject is responsible to ensure that the data he / she provides for processing and storage by the Company are accurate and up-to-date. Employees, customers, contractors and suppliers are required to notify the Company of any changes in circumstances so that Personal Data records can be updated.
The Company has a responsibility to ensure that any data change notification is recorded and appropriate action is taken.

Най-малко веднъж годишно администраторът преглежда сроковете на съхранение на всички лични данни, обработвани от Компанията и идентифицира всички данни, които вече не се изискват в контекста на регистрираната цел. Тези данни ще бъдат надеждно унищожени в съответствие с процедурите и правилата на администратора.

The Controller shall review the retention periods of all Personal Data processed by the Company at least once a year and shall identify any data that is no longer required in the context of the registered purpose. These data will be reliably destroyed in accordance with the Controller's procedures and rules.

Длъжностното лице по защита на данните отговаря в едномесечен срок на постъпило искане за корекция на данните.

The Data Protection Officer shall respond within one month to an individual's request to correct personal information.

Този срок може да бъде удължен с още два месеца, ако заявката е сложна или лицето е подало няколко заявки. Ако Компанията реши да не уважи с искането, Длъжностното лице по защита на данните уведомява писмено Субекта на данните за причините за отказа и за правото му да подаде жалба пред надзорния орган.

This period can be extended by a further two months if the request is complex or we have received a number of requests from the individual. If the Company decides not to comply with the request, the Data Protection Officer shall give a written notice to an individual, including the reasons for the refusal and the Data Subject's right to lodge a complaint with

Длъжностното лице по защита на данните ще предприеме всички разумни стъпки да информира организациите на трети страни, ако те обработват неточни или остарели лични данни и да препраща всяко искане за корекция на лични данни към третите страни, когато е необходимо.

Длъжностното лице по защита на данните трябва писмено да одобри всяко запазване на данни, което надхвърля определения срок на съхранение и да гарантира, че обосновката е ясно определена и е в съответствие с изискванията на законодателството за защита на данните.

4. Категории субекти на данни. Видове лични данни

„Зеебургер - информатик“ ЕООД обработва данни за следните категории субекти:

а) настоящи и бивши служители по трудово правоотношение - имена, ЕГН, дата на раждане, месторождение, номер и дата на издаване на лична карта, постоянен адрес, адрес за контакт (ако се различава от постоянния), снимки и видеоизображения, пол, данни за професионална квалификация и образование, телефонен номер и електронна поща за контакт, медицински данни (карта за предварителен медицински преглед, болнични листове, ТЕЛК решения), данни за съдимост (ако се изисква свидетелство за съдимост за заемане на длъжността), данни за членството в синдикални организации, данни за семейно положение, вкл. съпруг и деца, данни относно личен живот (начин на живот, навици и поведение), вътрешен (служебен) идентификационен номер, длъжност, възраст, трудов стаж, номер на банкова сметка, сума и причина за задължения към трети лица, информация за използването

the supervisory authority.

In case where third party organizations have inaccurate or outdated Personal Data, the Data Protection Officer shall take any reasonable steps to inform them that the information is inaccurate or out-of-date and, where necessary, forward any request for rectification of Personal Data to third parties.

The Data Protection Officer shall approve in writing any retention of Personal Data that exceeds the specified retention period and shall ensure that the reason is clearly defined and complies with the requirements of Data Protection Legislation.

4. Categories of Data Subjects. Types of Personal Data

Seeburger Informatik EOOD processes Personal Data about the following categories of data subjects:

a) current and former employees - names, PIN, date of birth, place of birth, identity card's number and date of issue, permanent address, contact address (if different from the permanent one), photos and video surveillance images, gender, information about a professional qualification and education, phone number and e-mail, medical data (preliminary medical examination card, sick notes, Territorial Medical Expert Panels (TMEP) decisions), criminal record data (if a criminal record certificate is required for the position), trade union membership data, marital status data, incl. a husband / spouse and children, personal life data (way of life, habits and behaviour), employee's identification number, job position, age, length of employment service, bank account number, amount and reason for employees` liabilities to third parties, information on the use of Company's information and communication systems;

на служебни информационни и комуникационни системи;

б) кандидати за работа - имена, дата на раждане, месторождение, адрес, телефон, ел. поща, снимка, данни за образованието и квалификацията, биографични данни, данни за семейно положение и други, които кандидатът е посочил в автобиография, мотивационно писмо или друг документ за подбор на персонал;

b) job applicants - names, date of birth, place of birth, address, phone number, e-mail, photo, information about a professional qualification and education, biographical data, marital status data and others which the job applicant has indicated in a CV, cover letter or other personnel selection document;

в) клиенти, контрагенти и доставчици на услуги - имена, ЕГН/ЛНЧ, дата на раждане, постоянен адрес, адрес за контакт (ако се различава от постоянния), телефон, ел. поща, банкова сметка, IP адрес, операционна система, браузър, информация за използването на служебни информационни и комуникационни системи (ако им е предоставен достъп), предоставени съгласия за приемане на политиката за поверителност и за ИТ сигурност;

c) customers, contractors and service providers - names, PIN/PNF, date of birth, permanent address, contact address (if different from the permanent one), phone number, e-mail, bank account, IP address, operating system, browser, information on the use of Company's information and communication systems (if access is granted), consents to the Company's Privacy Policy and IT security policy;

г) лица, работещи по граждански договор - имена, ЕГН/ЛНЧ или друг идентификационен номер, дата и място на раждане, адрес, степен на образование и професионални квалификации, банкова сметка, телефон, електронна поща, IP адрес, операционна система, браузър, информация за използването на служебни информационни и комуникационни системи (ако им е предоставен достъп), предоставени съгласия за приемане на политиката за поверителност и за ИТ сигурност;

d) individuals working under civil contract - names, PIN/PNF or other identification number, date of birth, place of birth, address, information about a professional qualification and education, bank account, phone number, e-mail, IP address, operating system, browser, information on the use of Company's information and communication systems (if access is granted), consents to the Company's Privacy Policy and IT security policy;

д) посетители в офиса на Компанията – имена, място на работа

e) visitors in the Company's premises – names, organisation name;

е) лични данни от видеонаблюдение – запис на изображения с времето, датата и местоположението за изброените в б. „а"-„д" лица.

f) Video Surveillance Personal Data – video-surveillance images with time, date and location stamp imposed on images for the individuals listed in letters "a" - "e" above.

5. Цел, основание и срок на обработването

Личните данни се събират единствено за конкретни, изрични и законни цели. Не се допуска Обработката на Лични данни за нови или различни цели или за цели, които са несъвместими с оповестените при първоначалното набиране на данните, освен в случаите, в които сме уведомили Субекта на данни за новите цели и, когато е необходимо, Субектът на данни е предоставил своето Съгласие.

5. Purpose, legal ground and retention period of the Processing

Personal Data are collected only for specific, explicit and lawful purposes. The Personal Data processing for new or different purposes or for purposes incompatible with those disclosed at the time of the initial data collection is not permitted, except in cases where we have notified the Data Subject of the new purposes and, where necessary, the Data Subject has given his / her Consent.

5.1. Личните данни на настоящи и бивши служители по трудово правоотношение се обработват:

а) цел – Компанията използва тези данни за сключване и изпълнение на трудовия договор, поддържане на трудовите досиета, спазване изискванията на трудовото, осигурителното и данъчното законодателство, изплащане на заплати, възнаграждения, обезщетения, бонуси и награди, предоставяне на социални придобивки, изчисляване и удържане на дължими данъци и осигуровки, за установяване, разследване, регистриране и отчитане на трудовите злополуки, за провеждане на периодични профилактични медицински прегледи, за осигуряване на достъпа на наетите лица до работните им места в съответствие с пропускателния охранителен режим, да се осигури безопасността на служителите, охрана на имущество, превенция и разкриване на престъпления, за изпълнение на задължение на Компанията като мрежова и информационна сигурност, предотвратяване на неоторизиран достъп до компютърните и електронните съобщителни системи на Компанията, както и предотвратяване на разпространението на злонамерен софтуер;

5.1. Processing of Current and Former Employees Personal Data:

a) purposes – Company uses these data to conclude and execute an employment contract, to maintain employment records, to comply with the requirements of labour, social security and tax legislation, to pay salaries, wages, benefits, bonuses and rewards, to provide social benefits, to calculate and withhold taxes and insurances due, for establishment, investigation, registration and reporting of occupational accidents, for conducting periodical preventive medical examinations, for ensuring the workplace access of the employees in accordance with the access security regime, for ensuring of staffs safety, protection of property, prevention and detection of criminal offences, for fulfilment of a Company's obligation as a jointly and severally liable third party liable under the Code of Civil Procedure, for conducting trainings, for ensuring Company's network and information security, for preventing unauthorized access to the computers and electronic communication systems of the Company, as well as preventing the spread of malicious software;

б) основания за обработването

b) legal grounds for processing

• Изпълнение на законово задължение: Кодекс на труда; Кодекс за социално осигуряване; Закон за здравното осигуряване; Закон за данъците върху доходите на физическите лица, Закон за здравословни и безопасни условия на труд, Граждански процесуален кодекс, Наредба № 4 от 11.05.1993 за документите, необходими за сключването на трудов договор, Наредба № 5 от 29.12.2002 за съдържанието и реда за изпращане на уведомлението по чл. 62, ал. 5 от Кодекса на труда, Наредба № Н-8 от 29.12.2005 за съдържанието, сроковете, начина и реда за подаване и съхранение на данни от работодателите, осигурителите за осигурените при тях лица, както и от самоосигуряващите се лица, Наредба за трудовата книжка и трудовия стаж, Наредба за медицинската експертиза, Наредба за паричните обезщетения и помощи от ДОО, Наредба за установяване, разследване, регистриране и отчитане на трудовите злополуки, Наредба № 3 от 18.04.2018 за условията и реда за откриване на платежни сметки, за изпълнение на платежни операции и за използване на платежни инструменти, Наредба № 3 от 28.02.1987 за задължителните предварителни и периодични медицински прегледи на работниците, Наредба № РД-07-2 за условията и реда да провеждането на периодично обучение и инструктаж на работниците и служителите по правилата за осигуряване на здравословни и безопасни условия на труд;

• Performance of a legal obligation: Labour Code; Social Insurance Code; Health Insurance Act; Income Taxes on Natural Persons Act; Health and Safety at Work Act; Code of Civil Procedure; Ordinance No 4 of 11.05.1993 on documents required for the conclusion of an employment contract; Ordinance No 5 of 29.12.2002 on the content and the procedure for submitting the notification under Art. 62, para. 5 of the Labour Code, Ordinance No N- 8 of 29.12.2005 on the content, terms, manner and procedure for submission and storage of insured persons' data by employers and social insurance contributors, as well as by self- insured persons, Ordinance on work book and length of employment service, Ordinance on medical expertise, Ordinance on cash benefits and allowances from public social insurance funds, Ordinance on the establishment, investigation, registration and reporting of occupational accidents, Ordinance No 3 of 18.04.2018 on the conditions and procedure for opening of payment accounts, for execution of payment transactions and for use of payment instruments, Ordinance No 3 of 28.02.1987 on the obligatory preliminary and periodical medical examinations of the workers, Ordinance No RD-07-2 on the terms and conditions for conducting periodical training and instruction of employees on the rules for ensuring healthy and safe working conditions;

• Изпълнение на договорно задължение: Трудови договори с персонала;

• Performance of a contract: Employment contracts with personnel;

• Легитимен (законен) интерес на Компанията: Видеонаблюдение и осигуряване на достъпа на наетите лица до работните им места в съответствие с пропускателния охранителен режим, наблюдение на начина на ползване на информационните и комуникационните системи на Компанията;

• Legitimate interest: Video surveillance. Ensuring the workplace access of the employees in accordance with the access security regime. Monitoring the use of the Company's information and communication systems;

• Съгласие на субекта: Изплащане на възнаграждения и обезщетения по банков път, за ползване на бонуси и социални придобивки, кандидатстване за работа или наемане на друг вид договор, за провеждане на обучения, за използване на снимки от корпоративни събития и обучения;

• Data Subject's Consent: To receive remuneration and benefits payments via bank transfer, as well as bonuses and social benefits, to apply for a job or to be hired another type of contract, for conducting trainings, for usage of photos from corporate events and trainings;

в) срок - трудов договор, заповеди за назначаване, преназначаване и прекратяване на трудовия договор, заповеди за ползване на неплатен отпуск до 30 дни годишно, ведомости за заплати, както и други документи, въз основа на които може да се установи трудов/осигурителен стаж - 50 години, считано от 1-ви януари на отчетния период, следващ отчетния период, за който се отнасят; болнични листове и други документи – 5 години, считано от 1-ви януари на годината, следваща годината на представянето им; счетоводни регистри и финансови отчети, включително документи за данъчен контрол, одит и последващи финансови инспекции – 10 години, считано от 1-ви януари на отчетния период, следващ отчетния период, за който се отнасят; данни за регистриране на трудови злополуки – 5 години от датата на регистрацията; документацията, отнасяща се до провеждането на обучение и инструктаж по безопасност и здраве при работа - 5 години; здравни досиета - 50 години; данни във връзка с достъп до работно място – 2 месеца; данни за членство в синдикални организации - 1 месец след получаване на уведомление от служителя, че е прекратил use of information and communication systems – 12 months; video-surveillance images with членството си, респ. 3 месеца след прекратяване на трудовото правоотношение; информация за използването на информационни
и комуникационни системи – 12 месеца; запис на изображения от видеонаблюдение с време, дата и местоположение – 2 месеца. До оттегляне на даденото съгласие, ако личните данни се обработват на това

c) retention periods – employment contract, orders for appointment, re-appointment and termination of the employment contract, orders for use of unpaid leave of up to 30 working days per year, payrolls, as well as other documents on the basis of which the length of employment service / contributory service can be established - 50 years from 1 January of the reporting period, following the accounting period to which they refer; sick notes и other documents – 5 years, reckoned from the 1st day of January of the year next succeeding the year they were presented; accounting records and financial statements, including documents for tax control, audit and subsequent financial inspections – 10 years from 1 January of the reporting period, following the accounting period to which they refer; data regarding to registration of occupational accidents – 5 years from the registration date; the documentation related to the conduct of training and instruction on safety and health in the workplace - 5 years; health records - 50 years; data related to access to the workplace – 2 months; trade union membership data - 1 month after receiving a notification from the employee that he / she has terminated the membership, resp. 3 months after termination of employment contract; information on the
time, date and location stamp imposed on images – 2 months. Where personal data are processed on the ground of consent, the processing ceases from the date of its withdrawal.

основание.

5.2. Личните данни на кандидати за работа се обработват:

а) цел - Компанията използва тези данни за подбор и назначаване на служители на работа на определени позиции, кадрово обезпечение на дейностите на Компанията;

б) основания за обработването
• Легитимен (законен) интерес на Компанията: Видеонаблюдение и осигуряване на достъп до офиса на Компанията в съответствие с пропускателния охранителен режим;
• Съгласие на субекта: дадено изрично или с конклудентни действия (подаване на документи за кандидатстване);

в) срок - 6 месеца съгласно чл. 25к от Закона за защита на личните данни или до оттегляне на съгласието, ако е оттеглено преди изтичане на този срок; запис на изображения от видеонаблюдение с време, дата и местоположение – 2 месеца.

5.2. Processing of Job Applicants Personal Data:

a) purposes - Company uses these data for selection and recruitment of employees to certain positions, staffing of the Company's activities;

b) legal grounds for processing
• Legitimate interest: Video surveillance. Ensuring the access to the Company's premises in accordance with the access security regime;

• Data Subject's Consent: given explicitly or by implied actions (submission of job application documents);

c) retention periods - 6 months according to Art. 25k of Personal Data Protection Act or until the consent is withdrawn where the withdrawal is made before the expiration of the retention period; video-surveillance images with time, date and location stamp imposed on images – 2 months.

5.3. Личните данни на клиенти, контрагенти и доставчици на услуги се обработват:
а) цел - Компанията използва тези данни, за да бъдат идентифицирани правилно страните, представляващите ги и лицата за контакт, да бъдат сключени и изпълнени задълженията по договорите с тях, да се осигури достъп в съответствие с безопасността на служители и външни посетители, охрана на имущество, превенция и разкриване на престъпления, за пропускателния охранителен режим, установен за Компанията, да се осигури осигуряване на мрежова и информационна сигурност, предотвратяване на неоторизиран достъп до компютърните и електронните съобщителни системи на Компанията, както и предотвратяване

5.3. Processing of Customers, Contractors and Service Providers Personal Data:

a) purposes - Company uses these data to verify the identity of the contracted parties, their representatives and contact persons; to conclude and fulfil the obligations under the contracts, to provide access in accordance with the access security regime established for the Company, to ensure staffs and visitors safety, to
protect Company's property and to prevent and detect criminal offences, to ensure the Company's network and information security, to prevent unauthorized access to the computers and electronic communication systems of the Company, as well as to prevent the spread of malicious software;

на разпространението на злонамерен софтуер;

б) основание за обработването
• Изпълнение на договорно задължение - сключения договор;
• Изпълнение на законово задължение – Закон за счетоводството, Закон за данък върху добавената стойност, Закон за корпоративното подоходно облагане;
• Легитимен (законен) интерес на Компанията - за сигурност и контрол на достъпа, както и за гарантиране на безопасността на персонала и посетителите, за защита на имуществото на компанията и за предотвратяване и откриване на престъпления, за наблюдение на начина на ползване на информационните и комуникационните системи на Компанията (ако е предоставен достъп до тях);

в) срок - 6 години, считано от 1-ви януари на годината, следваща годината, в която са прекратени или изпълнени продажбите/ доставките съгласно чл. 110 от Закона за задълженията и договорите във връзка със защитата на правата и интересите на дружеството при евентуални спорове; документи за данъчен контрол, одит и последващи финансови инспекции – 10 години, считано от 1-ви януари на отчетния период, следващ отчетния период, за който се отнасят; данни във връзка с достъп до офиса на Компанията – 2 месеца; информация за използването на информационни и комуникационни системи – 12 месеца; запис на изображения от видеонаблюдение с време, дата и местоположение – 2 месеца.

5.4. Личните данни на лица, работещи по граждански договор, се обработват:

а) цел - Компанията използва тези данни, за да бъдат идентифицирани правилно страните, да бъдат сключени и изпълнени задълженията по договорите

b) legal grounds for processing
• Performance of a contract – the concluded contract;
• Performance of a legal obligation – Accountancy Act, Value Added Tax Act, Corporate Income Tax Act;

• Legitimate interest - security and access control, ensuring of staffs and visitors safety, protection of Company's property, prevention and detection of criminal offences, monitoring the use of the Company's information and communication systems (if access is granted);

c) retention periods - 6 years, reckoned from the 1st day of January of the year next succeeding the year during which the sales / deliveries are terminated or executed according to Art. 110 of Obligations and Contracts Act in connection with the protection of the rights and interests of the Company in case of possible disputes; documents for tax control, audit and subsequent financial inspections – 10 years, reckoned from the 1st day of January of the reporting period, following the accounting period to which they refer; data relating to the access to the Company's premises – 2 months; information on the use of information and communication systems – 12 months; video - surveillance images with time, date and location stamp imposed on images – 2 months.

5.4. Processing of Personal Data of Individuals working under civil contract:

a) purposes - Company uses these data to verify the identity of the contracted parties, to conclude and fulfil the obligations under the contracts, to provide access in accordance

с тях, да се осигури достъп в съответствие с пропускателния охранителен режим, установен за Компанията, да се осигури безопасността на служители и външни посетители, охрана на имущество, превенция и разкриване на престъпления, за осигуряване на мрежова и информационна сигурност, предотвратяване н а неоторизиран достъп до компютърните и електронните съобщителни системи на Компанията, както и предотвратяване на разпространението на злонамерен софтуер;

with the access security regime established for the Company, to ensure staffs and visitors safety, to protect Company's property and to prevent and detect criminal offences, to ensure the Company's network and information security, to prevent unauthorized access to the computers and electronic communication systems of the Company, as well as to prevent the spread of malicious software;

б) основание за обработването

• Изпълнение на договорно задължение - сключения договор;

• Изпълнение на законово задължение – Кодекс за социалното осигуряване, Закон за данъците върху доходите на физическите лица, Наредба № Н-8 от 29.12.2005 г. за съдържанието, сроковете, начина и реда за подаване и съхранение на данни от работодателите, осигурителите за осигурените при тях лица, както и от самоосигуряващите се лица;

• Легитимен (законен) интерес на Компанията - за сигурност и контрол на достъпа, както и за гарантиране на безопасността на персонала и посетителите, за защита на имуществото на компанията и за предотвратяване и откриване на престъпления, за наблюдение на на начина на ползване на информационните и комуникационните системи на Компанията (ако е предоставен достъп до тях);

b) legal grounds for processing

• Performance of a contract – the concluded contract;

• Performance of a legal obligation – Social Insurance Code, Income Taxes on Natural Persons Act, Ordinance No N-8 of 29.12.2005 on the content, terms, manner and procedure for submission and storage of insured persons' data by employers and social insurance contributors, as well as by self-insured persons;

• Legitimate interest - security and access control, ensuring of staffs and visitors safety, protection of Company's property, prevention and detection of criminal offences, monitoring the use of the Company's information and communication systems (if access is granted);

в) срок - 6 години, считано от 1-ви януари на годината, следваща годината, в която е прекратен договора съгласно чл. 110 от Закона за задълженията и договорите във връзка със защитата на правата и интересите на дружеството при евентуални спорове; документи за данъчен контрол, одит и последващи финансови инспекции – 10 години, считано от 1-ви януари на

c) retention periods - 6 years, reckoned from the 1st day of January of the year next succeeding the year during which the contract is terminated according to Art. 110 of Obligations and Contracts Act in connection with the protection of the rights and interests of the Company in case of possible disputes; documents for tax control, audit and subsequent financial inspections – 10 years, reckoned from the 1st

отчетния период, следващ отчетния период, за който се отнасят; данни във връзка с достъп до офиса на Компанията – 2 месеца; информация за използването на информационни и комуникационни системи – 12 месеца; запис на изображения от видеонаблюдение с време, дата и местоположение – 2 месеца.

5.5. Личните данни на посетители в офиса на Компанията се обработват:

а) цел - Компанията използва тези данни за проверка на самоличността на посетителите, за сигурност и контрол на достъпа, както и за гарантиране на безопасността на персонала и посетителите, за защита на имуществото на компанията и за предотвратяване и откриване на престъпления;

б) основание за обработването - легитимен (законен) интерес;

в) срок - данни във връзка с достъп до офиса на Компанията – 2 месеца; запис на изображения от видеонаблюдение с време, дата и местоположение – 2 месеца.

5.6. Лични данни от видеонаблюдение

а) цел - Компанията използва своята система за видеонаблюдение единствено с цел сигурност и контрол на достъпа. Системата за видеонаблюдение помага за контрол на достъпа до помещенията и помага за гарантиране на защитата на инфраструктурата, безопасността на персонала и посетителите, както и защитата на собствеността и информацията, намираща се или съхранявана в помещенията. Тя е част от мерките, приети за укрепване на по-общите мерки, прилагани за целите на сигурността, и помага за предотвратяване, възпиране

day of January of the reporting period, following the accounting period to which they refer; data relating to the access to the Company's premises – 2 months; information on the use of information and communication systems – 12 months; video- surveillance images with time, date and location stamp imposed on images – 2 months.

5.5. Processing of Visitors' Personal Data:

a) purposes - Company uses these data for visitors' identity verification, security and access control, as well as to ensure staffs and visitors safety, to protect Company's property and to prevent and detect criminal offences;

b) legal ground for processing - a legitimate interest;

c) retention periods – data relating to the access to the Company's premises – 2 months; video-surveillance images with time, date and location stamp imposed on images – 2 months.

5.6. Processing of Video Surveillance Personal Data

a) purposes - Company uses its video- surveillance system for the sole purposes of security and access control. The video- surveillance system helps control access to the premises and helps to ensure the protection of the infrastructure, staff and visitor safety as well as the protection of the property and information located or stored on the premises. It forms part of the measures adopted to reinforce the more general measures applied for security purposes and helps to prevent, deter and if necessary detect any unauthorised physical access, including to areas placed under security or protection, IT infrastructure or

и, при необходимост, откриване на всеки неоторизиран физически достъп, включително до зони, поставени под сигурност или защита, ИТ инфраструктура или оперативна информация. В допълнение, видеонаблюдението помага за предотвратяване, откриване и разследване на кражби на оборудване или имущество, принадлежащи на Компанията, нейните посетители или персонал, или действия, застрашаващи безопасността на посетителите или персонала, работещ в помещенията (напр. пожари или физическо нападение);

operational information. In addition, video-surveillance helps prevent, detect and investigate the theft of equipment or property belonging to the Company, its visitors or staff or acts threatening the safety of visitors or staff working on the premises (fires or physical assault, for example);

б) основание за обработването - легитимен (законен) интерес;

b) legal ground for processing - a legitimate interest;

в) срок – 2 месеца съгласно чл. 56, ал. 4 от Закона за частната охранителна дейност. Записите се запазват за по-дълъг срок в случаите, когато е нужно за целите на разследване на престъпления или нарушения, за което Компанията уведомява разследващия орган – полиция, прокуратура, Комисия за защита на личните данни и др.
Достъп до данните от видеонаблюдение има единствено „Зеебургер - информатик“ ЕООД. Такъв достъп се предоставя и на компетентните държавни органи в предвидените в закон случаи. Физическите лица имат право на достъп до тези записи само в частта, която се отнася до тях. В случаите, когато при осъществяване правото на достъп на физическото лице могат да се разкрият лични данни и за трето лице, но няма техническа възможност за случаите, когато при осъществяване правото на достъп на физическото лице заличаване/маскиране на образите на другите лица-обект на видеонаблюдението, достъп до видеозаписи може да бъде предоставен само със съгласието на всички лица-обект на видеонаблюдението.

c) retention period – 2 months according to Art. 56, para. 4 of Private Security Business Act. The records may be kept for a longer period in cases where it is necessary for the purposes of investigation of criminal offences or breaches, for which the Company notifies the relevant investigating body - police, prosecutor's office, Commission for Personal Data Protection and others.
Only Seeburger Informatik EOOD has access to video surveillance data. Such access shall also be granted to the competent state authorities in the cases provided by law. Individuals have the right to access these data only insofar as they relate to them. In cases where the exercise of the natural person's right of access may disclose third party's personal data, but there is no technical possibility to erase or mask the images of other persons subject to video surveillance, access to video recordings / images may be granted only with the consent of all individuals subject to video surveillance.

„Зеебургер - информатик“ ЕООД е

Seeburger Informatik EOOD is a Controller

администратор на данни, а в някои случаи - обработващ съгласно Регламент (ЕС) 2016/679. Когато Компанията обработва лични данни в качеството ѝ на Обработващ, категориите субекти на данни, видовете лични данни, целта, основанието и срока на обработване се определя от Администратора, който е възложил обработването.

and in some cases a Processor in accordance with GDPR. Where the Company processes Personal Data in its capacity as Processor, the categories of data subjects, the types of Personal Data, the purposes, the grounds and the period of processing are determined by the Controller who has assigned the processing.

6. Сигурност и защита на личните данни

Сигурността на личните данни е наш приоритет, с който не правим никакви компромиси.
Личните данни следва да бъдат защитени посредством подходящи технически и организационни мерки срещу неупълномощена и л и незаконна Обработка, както и срещу или незаконна загуба, унищожаване, промяна, оповестяване или увреждане.
„Зеебургер - информатик“ ЕООД е въвел разумни и подходящи мерки за сигурност срещу незаконната или неупълномощена Обработка на Лични данни, както и срещу случайната загуба или увреждане на Лични данни. Компанията полага особена грижа за защитата на Чувствителни лични данни от загуба или неупълномощен достъп, употреба или оповестяване.

6. Personal Data Security and Protection

The Personal Data security is our priority that we never compromise on.
Personal Data should be protected by appropriate technical and organizational measures against unauthorized or unlawful processing and against accidental or unlawful loss, destruction, alteration, disclosure or damage.

Seeburger Informatik EOOD has implemented reasonable and appropriate security measures against unlawful or unauthorized Personal Data processing and against accidental loss or damage of Personal Data. The Company gives special attention to Sensitive Personal Data protection from loss or unauthorized access, use or disclosure.

В „Зеебургер - информатик“ ЕООД е внедрена Система за управление на информационната сигурност (Information Security Management System - ISMS) в съответствие с международния стандарт ISO/IEC 27001:2013.

Seeburger Informatik EOOD has implemented an Information Security Management System (ISMS) in accordance with the international standard ISO/IEC

Спазването на изискванията на стандарта се одитира и сертифицира ежегодно. Защитите, които се изградени в компанията при внедряване на СУИС, гарантират осигуряването и поддържането на много високо ниво на сигурност на данните, както и поверителността, наличността и целостта на информацията (confidentiality, availability

The compliance with the requirements of this standard is audited and certified annually. The safeguards that are built in the company during the implementation of ISMS ensure the provision and maintenance of a very high level of data security, as well as confidentiality, availability and integrity of the information, including the Personal Data.

and integrity), в т.ч. и на Личните данни.

В допълнение към Системата за управление на информационната сигурност и с цел контролиране на спазването на вече внедрените изисквания за осигуряване на информационната сигурност, компанията е внедрила и текущо развива Вътрешна контролна система (Internal control system - ICS), която е базирана на ISAE 3402 (SOC 1). Тази система също се одитира и оценява всяка година (SOC 1 Type 2 Examination).

In addition to the Information Security Management System and in order to control the compliance with the already implemented requirements for information security, the Company has implemented and is currently developing an Internal Control System (ICS), which is based on ISAE 3402 (SOC 1). This system is also audited and evaluated annually (SOC 1 Type 2 Examination).

Всички служители са отговорни за гарантирането на сигурността при съхраняването на данните, за които те отговарят и които „Зеебургер - информатик" ЕООД държи, както и, че данните се съхраняват сигурно и не се разкриват при каквито и да било обстоятелства на трети страни, освен ако Компанията не е дала такива права на тази трета страна и има сключен договор/клауза за поверителност с дружеството. Допуска се трансфер на Лични данни до трети лица – доставчици на услуги, ако са поели договорен ангажимент да спазват нашите политики и процедури, и които са се ангажирали да въведат адекватни мерки за защита на Личните данни. въведени с цел поддържане на сигурността на всички Лични данни от момента Служителите са длъжни да спазват всички политики, процедури и технологии, 27001:2013. събирането им до момента на унищожаването им. Всички служители са запознати с нашите IT security и GDPR документи, които са задължителни за тях. Документите са публикувани във вътрешната мрежа на компанията - info. seeburger.de – и са достъпни за всички служители.

All employees shall ensure the security of the data storage for which data they are responsible for and which Seeburger Informatik EOOD holds, as well as that the data are stored securely and are not disclosed under any circumstances to third parties, except where the Company has granted such rights to this third party and has a contract/confidentiality clause with it. Personal Data transfer to third parties - service providers is allowed, if they have made a contractual commitment to comply with our policies and procedures, and have committed to implement adequate measures for Personal Data protection.
Employees are obliged to comply with all policies, procedures and technologies in place to maintain the security of all Personal Data from the time they are collected until they are destroyed. All employees are familiar with our IT security and GDPR documents, which are mandatory for them. The documents are published on the Company's internal network - info.seeburger.de - and are available to all employees.

Служителите имат достъп само до информацията, която тяхната длъжност изисква в съответствие с принципа „необходимост да се знае", а достъпът може да бъде предоставен само в съответствие с

Employees have access only to the information that their job function requires in accordance with the need-to-know principle and the access can only be granted in accordance with the rules for access control. All Personal Data

правилата за контрол на достъпа. Всички Лични данни се третират с найголяма сигурност и се съхраняват:
• в самостоятелна стая с контролиран достъп и в заключващи се шкафове, които са достъпни само за служителите, работещи в стаята; и/или
• ако са компютъризирани са защитени с парола в съответствие с вътрешните изисквания, посочени в съответните политики на ИТ сигурност.

are treated with extra security and stored:

• in a separate room with controlled access and in lockable containers, accessible only to the employees working in the room; and / or
• if they are computerized they are password protected in accordance with the internal requirements specified in the relevant IT security policies.

От всички служители се изисква да бъдат обучени и да приемат съответните договорни клаузи/декларация за поверителност и спазване на политиките за ИТ сигурност, както и правилата за заключване на работните станции, преди да им бъде предоставен достъп до информация от всякакъв вид.
Записите върху хартиен носител не трябва да се оставят там, където могат да бъдат достъпни от неоторизирани лица и не могат да бъдат изваждани от определените офисни помещения без изрично разрешение. Веднага щом хартиените документи вече не са необходими за текущата работа, те трябва да бъдат унищожени в съответствие със създадена за това процедура/правила и съответен протокол.

All employees are required to be trained and to accept the relevant contractual clauses / Privacy and IT security policies compliance Statement, as well as the rules for locking workstations, before they are granted access to information of any kind.
Paper-based records should not be left where they can be accessed by unauthorized persons and cannot be removed from designated office premises without express permission. As soon as the paper documents are no longer needed for the current work, they must be destroyed in accordance with the implemented procedure / rules and appropriate protocol.
Personal Data may be erased or destroyed only in accordance with the Data Retention and Destruction Procedure. Paper-based records that have reached its retention date should be shredded and disposed of as confidential waste.

Личните данни могат да бъдат изтривани или унищожавани само в Записите на хартиен носител, които са достигнали датата на съхранение, трябва да бъдат нарязани и унищожени като "поверителни отпадъци". Данните върху твърдите дискове на излишните персонални компютри трябва да бъдат изтрити или дисковете унищожени, съгласно внедрените правила/процедури.

The data on the hard disks of the redundant personal computers must be erased or the disks destroyed according to the implemented rules / procedures. The Personal Data processing off office poses a potentially higher risk of loss, theft or breach of personal data. Staff members must be explicitly authorized to process data off the Controller's premises.

Обработването на лични данни "извън офиса" представлява потенциално по-голям риск от загуба, кражба или нарушение на

In determining the appropriateness of the processing, shall be taken into account the degree of possible damage or loss that may

лични данни. Персоналът трябва да бъде специално упълномощен да обработва данните извън обекти на администратора.

be caused to individuals if a security breach occurs, as well as any likely types of damage to the Controller's reputation, including any loss of customers / contractors confidence.

При определянето на това доколко уместно е обработването се вземат предвид степента на евентуална вреда или загуба, която може да бъде причинена на физически лица, ако възникне нарушение на сигурността, както и всяка вероятна вреда за репутацията на администратора, включително евентуална загуба на доверие на клиентите/контрагентите.
При оценяването на подходящи технически мерки се взема предвид:
• защита с парола;
• автоматично заключване на бездействащи работни станции в мрежата;
• премахване на права на достъп за USB и други преносими носители с памет;
• антивирусен софтуер и защитни стени;
• правата за достъп, основани на роли;
• защита на устройства, които напускат помещенията на Компанията, като лаптопи, таблети или други;
• сигурност на локални и широкообхватни мрежи;
• технологии за подобряване на поверителността, като например псевдонимизиране и анонимизиране;
• идентифициране на подходящи международни стандарти за сигурност, подходящи за Компанията.

Upon evaluating the appropriate technical measures the following shall be taken into account:
• password protection;
• automatic lock of workstations in the network after a period of inactivity;
• removal of access rights for USB and other removable storage media;
• antivirus software and firewalls;
• role-based user access;
• protection of devices leaving the Company's premises (e.g. laptops, tablets, etc.);
• security of local and wide area networks;
• confidentiality enhancement technologies, such as pseudonymization and anonymization;
• identification of appropriate international security standards appropriate for the Company.

При оценяването на подходящите организационни мерки се взема предвид:
• нивата на подходящо обучение в Компанията;

Upon evaluating the appropriate organizational measures the following shall be taken into account:

• мерките, които отчитат надеждността на служителите (например атестационни оценки, препоръки и т.н.);
• включването на защитата на данните в трудовите договори;
• идентификация на дисциплинарни мерки за нарушения по отношение на

• the levels of the relevant training in the Company;
• employees' reliability measures (e.g. attestations, recommendations, etc.);
• inclusion of data protection clauses in the employment contracts;
• identification of disciplinary measures for

обработването на данни;
• редовна проверка на персонала за спазване на съответните стандарти за сигурност;
• контрол на физическия достъп до електронни и хартиено базирани записи;
• приемане на политика на „чисто работно място“1;
• съхраняване на хартиени бази данни в заключващи се шкафове;
• ограничаване на използването на портативни електронни устройства извън работното място;
• ограничаване на използването от служителите на лични устройства на работното място;
• приемане на ясни правила за създаване и ползване на пароли;
• редовно създаване на резервни копия на личните данни и физическо съхраняване на носителите с копия извън офиса;
• налагане на договорни задължения на организации контрагенти да предприемат подходящи мерки за сигурност при прехвърляне на данни.

the breaches of Personal Data processing;
• regular inspection of personnel for compliance with the relevant security standards;
• physical access control to electronic and paper-based records;
• implementation of Clean Desk Policy1;
• storage of paper-based data in lockable containers;
• restriction of use of portable electronic devices outside the workplace;
• restriction of use of employees` portable devices in the workplace;
• adoption of clear rules for creating and using passwords;
• regular backup of personal data and physical storage of media copies outside the office;
• imposition of contractual obligations on counterparty orgnizations to take appropriate security measures when transferring data.

При напускане на работното място, всички документи и бележки, вкл. лепящи се бележки, визитни картички и преносими устройства (като USB флаш памет) се премахват или прибират в места с ограничен достъп - специални заключващи се шкафове, заключени помещения, унищожаване на вече ненужни документи и т.н.

Upon leaving the working place, all documents and notes, including any post-it notes, businesses cards, and removable media (e.g. USB memory sticks) are removed or stored in places with limited access - lockable storage boxes, locked rooms, destruction of unnecessary documents, etc.

7. Разкриване на лични данни

„Зеебургер - информатик“ ЕООД осигурява условия, при които личните данни не се разкриват на неупълномощени трети страни, което включва членове на семейството, приятели, държавни органи, дори разследващи такива, ако има основателно съмнение, че не се изискват по установения ред. Всички служители трябва да бъдат предпазливи, когато им поискат

7. Disclosure of Personal Data

Seeburger Informatik EOOD provides conditions under which Personal Data shall not be disclosed to unauthorized third parties, including family members, friends, government agencies, even investigators, if there is reasonable doubt that the Personal Data are not requested in the prescribed manner. All employees must be careful when they are asked to disclose Personal Data of another person

да разкрият съхранявани лични данни за друго лице на трета страна. Важно е да се има предвид, дали разкриването на информацията е свързано или не с нуждите на дейността, извършвана от институцията. На служителите следва да се извършва специално обучение и периодични инструктажи с цел да се избегне рискът от такова нарушение.
Всички искания от трети страни за предоставяне на данни трябва да бъдат подкрепени с подходяща документация и всички такива разкривания на данни трябва да бъдат специално разрешени от Длъжностното лице по защита на данните.

to the third party. It is important to consider whether or not the disclosure is related to the activity carried out by the institution.
Employees should receive special training and periodic briefings in order to avoid the risk of such a breach.
All Personal Data disclosure requests from third parties shall be supported by appropriate documentation, as well as all such disclosure requests must be specifically authorized by the Data Protection Officer.

8. Съхраняване и унищожаване на данните

„Зеебургер - информатик“ ЕООД не съхранява лични данни във вид, който позволява идентифицирането на субектите за по-дълъг период отколкото е необходимо, по отношение на целите, за които са били събрани данните.
Периодът на съхранение за всяка категория лични данни се определя съобразно законовите изисквания, а когато няма изрично регламентирани законови срокове се използват ясни критерии за определяне на този период.
Длъжностното лице по защита на данните определя периода от време, през който трябва да се съхраняват документите и електронните записи. Компанията и нейните служители редовно преглеждат всички данни, независимо дали се съхраняват по електронен път на тяхното устройство или на хартия, за да решат дали да унищожат или изтрият данни, след като целта, за която са създадени тези документи, вече не е от значение.

8. Data Retention and Destruction

Seeburger Informatik EOOD does not store Personal Data in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data are collected.
The retention period for each type of Personal Data is determined in accordance with the legal requirements. Where no explicitly regulated legal deadlines are set out, clear criteria are used to determine this period.
The Data Protection Officer defines the time period for which the documents and electronic records should to be retained. The Company and its employees shall, on a regular basis, review all data, whether held electronically on their device or on paper, to decide whether to destroy or delete any data once the purpose for which those documents were created is no longer relevant.

„Зеебургер - информатик“ ЕООД може да съхранява данни за по-дълги периоди единствено ако личните данни ще бъдат обработвани за целите на архивиране, за цели в обществен интерес, научни или

Seeburger Informatik EOOD may keep Personal Data for longer periods insofar as the Personal Data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statis-

исторически изследвания и за статистически цели, и само при изпълнението на подходящи технически и организационни мерки за гарантиране на правата и свободите на Субекта на данните. Личните данни трябва да бъдат унищожени сигурно, съгласно принципа за гарантиране 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. Данните трябва да бъдат изтрити, нарязани или унищожени по друг начин до степен, еквивалентна на тяхната стойност за другите и тяхното ниво на поверителност.
Длъжностното лице по защита на данните документира и одобрява процеса на унищожаване на данните.

tical purposes and if an appropriate technical and organisational measures are implemented in order to safeguard the rights and freedoms of the Data Subject.
Personal Data must be destroyed securely in accordance with the principle of ensuring an adequate level of security, including protection against unauthorized or unlawful processing, accidental loss, destruction or damage, by applying appropriate technical or organizational measures. The data should be deleted, shredded or otherwise destroyed to a degree equivalent to their value to others and their level of confidentiality.
The Data Protection Officer shall fully document and approve the destruction process.

9. Ограничение на трансферите на данни

Лични данни се считат за трансферирани, когато произхождат от една държава и бъдат предадени, изпратени, разглеждани или до данните е осъществен достъп (включително дистанционно) в друга държава.

С цел да се гарантира, че нивото на защита на данните не е компрометирано, Личните данни не бива да са трансферират извън ЕИП, освен когато са въведени подходящи мерки за защита (напр. споразумение за трансфер, основаващо се на стандартни договорни клаузи). Всеки трансфер на Лични данни извън ЕИП подлежи на предварително писмено одобрение от Длъжностното лице по защита на данните.

По изключение, „Зеебургер - информатик“ ЕООД може да прехвърля лични данни в държави членки на ЕС или в трета страна или международна организация само при едно от следните условия:

9. Data Transfer Restrictions

Personal Data are considered to be transferred when they originate in one country and are transmitted, sent, viewed or accessed (including remotely) in another country.

In order to ensure that the level of data protection is not compromised, Personal Data should not be transferred outside the EEA, unless appropriate protection measures are in place (e.g. a data transfer agreement based on standard contractual clauses). Any transfer of Personal Data outside the EEA is subject to prior written approval by the Data Protection Officer.

Exceptionally, Seeburger Informatik EOOD may transfer Personal Data to EU Member States or to a third country or international organization only under one of the following conditions:

• субектът на данните изрично е поискал прехвърляне, след като е бил информиран за възможните рискове от такива прехвърляния;
• предаването е необходимо за изпълнението на договор между Субекта на данните и администратора/обработващия или за изпълнението на преддоговорни мерки, взети по искане на Субекта на данните;
• предаването е необходимо поради важни причини от обществен интерес;
• предаването е необходимо за установяването, упражняването или защитата на правни
претенции;
• предаването е необходимо, за да бъдат защитени жизненоважните интереси на Субекта на данните или на други лица, когато Субектът на данните е физически или юридически неспособен да даде своето съгласие.

За да се гарантира, че личните данни получават адекватно ниво на защита, ние имаме или ще приложим споразумения за прехвърляне на лични данни с включени в тях клаузи, съответстващи на модел, приет от Европейската комисия или по друг начин, за да се осигури адекватното ниво на защита, така че да сте сигурни, че личните данни се обработват от тези трети страни по начин, който е в съответствие с приложимото европейско законодателство за защита на личните данни.

• the Data Subject has explicitly requested a transfer after being informed of the possible risks of such transfers;
• the transfer is necessary for the performance of a contract between the Data Subject and the Controller / Processor or the implementation of pre-contractual measures taken at the Data Subject's request;
• the transfer is necessary for important reasons of public interest;
• the transfer is necessary for the establishment, exercise or defence of legal claims;
• the transfer is necessary in order to protect the vital interests of the Data Subject or of other persons, where the Data Subject is physically or legally incapable of giving consent.

In order to ensure that Personal Data have an adequate level of protection, we have or will implement data transfer agreements, corresponding to a model adopted by the European Commission or other instrument to ensure an adequate level of protection, so that you can be sure that Personal Data are processed by these third parties in a way that is in line with applicable European data protection legislation.

10. Докладване на нарушения на сигурността на Личните данни

При определени обстоятелства, „Зеебургер - информатик" ЕООД е длъжен да докладва за нарушения на сигурността на Личните данни към надзорния орган за защита на данните и, в някои случаи, към Субекта на данни.

ОРЗД задължава администратора да

10. Personal Data Breach Notification

In certain circumstances, Seeburger Informatik EOOD is obliged to report Personal Data breaches to the supervisory authority and, in some cases, to the Data Subject.

The GDPR introduces a duty on the Controller

уведоми за нарушение компетентния надзорен орган, освен ако липсва вероятност нарушението да породи риск от настъпването на неблагоприятни последици за правата и свободите на физическите лица. Когато има голяма вероятност и риск да настъпят тези неблагоприятни последици, ОРЗД задължава администратора да уведоми за нарушението засегнатите физически лица без излишно забавяне.

to report Personal Data breaches to the relevant supervisory authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where there is a high probability and risk of adverse effects occurring, the GDPR obliges the Controller to notify the affected individuals without undue delay.

Въвели сме специална Политика, за да се справим с всякакви съмнения за нарушения на сигурността на личните данни и ще уведомяваме Субектите на данни и/или приложимия регулатор в случаите, в които имаме законовото задължение за такова докладване.

We have implemented a special Policy to deal with any suspected breaches of personal data security and will notify the Data Subjects and / or the relevant supervisory authority in cases where we have a legal obligation to do so.

11. Права и искания на Субекта на данни

11. Data Subject's Rights and Requests

Субектите на данни, намиращи се в ЕС, имат определени права по отношение на обработването на Личните им данни.
ОРЗД предоставя на физическите лица следните права:

All Data Subjects located in the EU have certain rights with regard to the processing of their Personal Data.
The GDPR provides individuals with the following rights:

(а) да поискат информация за това дали съхраняваме техни Лични данни, като в случай, че имаме такива – какви са тези данни, на какво основание и с каква цел ги обработваме и съхраняваме;

(a) to demand information on whether we store their personal data, and if so, what data we collected, what are our legal grounds for processing them and for what purpose we process and store their data;

(б) да поискат достъп до Личните си данни (т.нар. "заявка за достъп до данни"). Това им позволява да получат копие от Личните данни и да проверят дали ги обработваме по установения по закон начин;

(b) to request access to their Personal Data (the so-called `Data Subject access request`). This allows them to obtain a copy of the Personal Data and to check whether we are processing them in the manner prescribed by law;

(в) да поискат коригиране на притежаваните от нас техни Лични данни, ако те са непълни или неточни;

(c) to request the rectification of incomplete or inaccurate their Personal Data held by us;

(г) да поискат изтриване на техните Лични данни (т.нар. „право да бъдеш забравен"), т.е. да изтрием или премахнем без излишно забавяне всички или част от техните лични данни, ако Личните данни повече

(d) to request the erasure of their Personal Data (the so-called `right to be forgotten`), i.e. to delete or remove without undue delay all or part of their Personal Data, if the Personal Data are no longer necessary in relation to

не са необходими за целите, за които са били събрани или обработвани по друг начин. Компанията не изтрива данните, когато обработването е в изпълнение на законово задължение, включително за установяването, упражняването или защитата на правни претенции;

the purposes for which they were collected or otherwise processed. The Company does not erase the data where the processing is necessary for compliance with a legal obligation, including for the establishment, exercise or defence of legal claims;

(д) да възразят срещу обработването на техни Лични данни, в случай че се позоваваме на легитимен интерес (или интересите на трета страна) или за директни маркетингови цели;

(e) to object to the processing of their Personal Data if we invoke a our legitimate interest (or the interests of a third party) or where the Personal Data are processed for direct marketing purposes;

(е) да поискат да изтрием или премахнем техни Лични данни, ако са упражнили правото си да възразят срещу обработването им съгласно предходната буква;

(f) to request the erasure or removal of their Personal Data if they have exercised their right to object to the processing in accordance with the preceding letter (e);

(ж) да възразят срещу автоматичното вземане на решения, ако се извършва такова, включително профилиране, т.е. да не бъдат обект на никакво автоматизирано вземане на решения от нас посредством Личните им данни или профилиране;

(g) to object to any decision-making based solely on automated processing, if any, including profiling, i.e. not to be subject to any automated decision-making by us through their Personal Data or profiling;

(з) да поискат ограничаване на обработването на техни Лични данни, т.е. да преустановим обработването им, ако например субектът желае да установим верността им или причината за обработването им;

(h) to request a restriction of the processing of their Personal Data, i.e. to suspend their processing if, for example, the Data Subject wishes to verify their accuracy or the purposes of their processing;

(и) да получат Личните си данни в структуриран, широко използван и пригоден за машинно четене формат (т.нар. „право на преносимост на данните“). Това позволява да вземат данните си от Компанията и да ги прехвърлят на друг администратор;

(i) to receive their Personal Data in a structured, commonly used and machine-readable format (the so-called `right to data portability`). This allows them to take their data from the Company and to transmit those data to another controller;

(й) да оттеглят даденото си съгласие. Може да се оттегли съгласието за всички или само за част от Личните данни, както и за конкретна или за всички цели на обработване. Ако субектът е дал съгласие

(j) to withdraw their Consent. The Consent may be withdrawn for all or part of the Personal data, as well as for all or specific purposes of processing. Where the Data Subject has given his / her Consent for the collection, pro-

за събиране, обработване и съхраняване на Личните му данни за определена цел, има право по всяко време да го оттегли относно този конкретен вид обработване. След като бъдем уведомени за оттегляне на съгласието, ние ще преустановим обработването им за целта или целите, за които е предоставено съгласието, освен ако не съществува друго основание да продължим тази обработка;

cessing and storage of his / her Personal data for a specific purpose, he /her has the right to withdraw it at any time in respect of that particular type of processing. Once we have been notified of the withdrawal of Consent, we will suspend their processing for the purpose or purposes for which the consent was granted, unless there is another legal basis for continuing to process them;

(к) да бъдат уведомени в случай на нарушение на сигурността на техните Лични данни, което може да породи висок риск за техните права и свободи. При установяване на такова нарушение Компанията ще информира субектите без излишно забавяне и по подходящ начин, както и за мерките, които са предприети или предстои да бъдат предприети.

(k) to be notified in the case of a Personal Data Breach, which may result in a high risk to their rights and freedoms. After having become aware of a Personal Data Breach, the Company will inform the individuals without undue delay and in an appropriate manner, as well as the measures that have been taken or the measures that will be taken.

„Зеебургер - информатик“ ЕООД осигурява условия, които да гарантират упражняването на тези права от субекта на данни като същите са подробно описани в Политика за искания за достъп до данни на субект.
За да упражни някое от изброените по-горе права, субектът на данни следва да изпрати искане или уведомление в свободен текст по пощата на адрес: **гр. София, п.к. 1797, район Изгрев, бул. „Д-р Г. М. Димитров“ № 16-А или на e-mail: dpo.bg@seeburger.com.**

Seeburger Informatik EOOD ensures conditions that guarantee the exercise of the Data Subject Rights. These conditions are described in detail in our Data Subjects Access Request Policy.
In order to exercise any of the above rights, the Data Subject should send a free text request or notification by post at the following address: **16-A D-r G. M. Dimitrov Blvd., "Izgrev" district, 1797 Sofia city or via e-mail dpo.bg@seeburger.com.**

Зеебургер - информатик“ ЕООД може да поиска от субекта на данни конкретна информация, за да бъде потвърдена самоличността му и да бъде уважено правото му за достъп до информация или някое от останалите му права. Целта на тази допълнителна мярка за сигурност е да гарантира, че личните данни на субекта няма да бъдат разкрити пред лица, които нямат право да ги получат.
Упражняването на посочените по-горе права не изисква заплащането на

Seeburger Informatik EOOD may request specific information from the Data Subject in order to verify his / her identity and to satisfy his / her right to access information or any of his / her other rights. The purpose of this additional security measure is to ensure that the Data Subject's Personal Data shall not be disclosed to persons who are not entitled to receive them.
The exercise of the above rights is free of charge. However, we may ask a reasonable amount of administrative fee if the access

такса. Възможно е да бъде начислена административна такса в разумен размер, ако заявката за достъп е очевидно необоснована или при повторяемост или прекомерност на исканията. При подобни обстоятелства е възможно също така да бъде отказано изпълнението на заявката.
Ако субектът на данни смята, че правата за защита на личните му данни са били нарушени, има право да подаде жалба до Комисията за защита на личните данни на адрес **гр. София 1592, бул. „Проф. Цветан Лазаров" № 2 или по електронна поща kzld@cpdp.bg.**

request is manifestly unfounded or if the requests are repeated or excessive. In this cases, it is also possible to refuse the execution of the request.
If the Data Subject considers that his / her data protection rights have been breached, he / she has the right to lodge a complaint with the Commission for Personal Data Protection at the following address: **2 Prof. Tsvetan Lazarov Blvd., Sofia 1592 or via e-mail kzld@cpdp.bg.**

12. Съгласие на субекта на данните

„Зеебургер - информатик" ЕООД разбира под "съгласие" само случаите, в които Субектът на данните е бил напълно информиран за планираното обработване и е изразил своето съгласие свободно, без да му бъде упражняван натиск. Съгласието, получено при натиск или въз основа на подвеждаща информация, няма да бъде валидно основание за обработване на лични данни.
Съгласието не може да бъде изведено от липсата на отговор на съобщение до Субекта на данни. Трябва да има активна комуникация между администратора и субекта, за да е налице съгласие. В случаите, когато основанието за обработване на данните е съгласие на субекта, администраторът задължително изисква формуляр за съгласие.

12. Consent of the Data Subject

Seeburger Informatik EOOD considers that there is "a consent" only in cases where the Data Subject has been fully informed of the intended processing and has freely expressed his / her consent without being pressured. Consent obtained under duress or on the basis of misleading information will not be a valid basis for the Personal Data Processing.
The Consent cannot be inferred from a lack of response to a message to the Data Subject. There must be active communication between the Controller and the Data Subject to assume that there is consent. In case where the legal ground for data processing is the consent of the Data Subject, the Controller shall require a consent form.

13. Промени в настоящата Политика за поверителност

Настоящата Политика за поверителност ще се преглежда и актуализира редовно в съответствие със задълженията ни за защита на данните, като си запазваме правото периодично да я изменяме или допълваме. Новата или изменена политика ще бъде разпространена до всички Членове на персонала веднага щом бъде приета.

13. Privacy Policy Changes

This Privacy Policy will be reviewed and updated regularly in accordance with our data protection obligations, and we reserve the right to periodically amend or supplement it. Each new Policy or change of this Policy will be circulated to all Staff Members as soon as it is adopted.

SEEBURGER
BUSINESS INTEGRATION

Декларация за получаване и преглед

Аз, (име) декларирам, че на (дата) получих и прочетох копие от Политиката за поверителност на „Зеебургер-информатик" ЕООД, и съм наясно, че нося отговорност за познаването и спазването на нейните условия.

Подпис:.....

Име:.....

Receipt and Review Declaration

I, (name) hereby declare that on this date of I rceived and read a copy of the Privacy Policy of Seeburger Informatik EOOD, and I am aware of my responsibility for knowing and complying with its terms.

Signature:.....

Name:.....

Приложение А Определения

Администратор: всяко физическо или юридическо лице, публичен орган, агенция или друга структура, която сама или съвместно с други определя целите и средствата за обработването на лични данни. Когато целите и средствата за това обработване се определят от правото на ЕС или правото на държава членка, администраторът или специалните критерии за неговото определяне могат да бъдат установени в правото на Съюза или в правото на държава членка.

Получател: физическо или юридическо лице, публичен орган, агенция или друга структура, пред която се разкриват личните данни, независимо дали е трета страна или не. Същевременно публичните органи, които могат да получават лични данни в рамките на конкретно разследване в съответствие с правото на ЕС или правото на държава членка, не се считат за „получатели"; обработването на тези данни от посочените публични органи отговаря на приложимите правила за защита на данните съобразно целите на обработването.

Трета страна: всяко физическо или юридическо лице, публичен орган, агенция или друг орган, различен от субекта на данните, администратора, обработващия лични данни и лицата, които под прякото

APPENDIX A – DATA PROTECTION TERMS

Data Controller or Controller: any natural person or legal entity, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. Where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Recipient: any natural person or legal entity, public authority, agency or other body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.

Third party: any natural person or legal entity, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to pro-

ръководство на администратора или на обработващия лични данни имат право да обработват личните данни.

Съгласие: свободно дадено, конкретно, информирано и недвусмислено заявление за съгласие от страна на Субекта на данни, посредством което, по силата на декларация или ясно позитивно действие, същият предоставя съгласието за Обработката на свързани с него Лични данни.

Субект на данни: жив, идентифициран или идентифицируем индивид, относно който обработваме Лични данни, и който се намира в рамките на ЕС, или чиито Лични данни другояче подлежат на защита от европейските закони за защита на данните. Субект на данни е физическо лице, което може да бъде идентифицирано по- специално чрез идентификатор като име, идентификационен номер, данни за местонахождение, онлайн идентификатор или по един или повече признаци, специфични за физическата, физиологичната, генетичната, психическата, умствената, икономическата, културната или социална идентичност на това физическо лице.

ЕИП: 27-те държави на ЕС, както и Исландия, Лихтенщайн и Норвегия.
Изрично съгласие: съгласие, което изисква много ясно и конкретно писмено заявление (а не само действие).

Лични данни: всякаква информация, която идентифицира Субект на данни, или информация отнасяща се до Субект на данни, когото можем да идентифицираме (пряко или непряко) въз основа единствено на тези данни или в комбинация с други идентификатори, които притежаваме или до които разумно бихме могли да получим достъп. Личните данни не включват анонимизирани данни или данни, в които идентичността на индивида е трайно отстранена. Личните данни могат да бъдат

cess personal data.

Consent: any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Data Subject: a living identified or identifiable individual about whom we process Personal Data and who is located within EU, or whose Personal Data is otherwise subject to protection by EU data protection legislation. A Data subject is a natural person who can be identified in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, intellectual, economic, cultural or social identity of that natural person.

EEA: 27 Member States of the EU, as well as Iceland, Liechtenstein, and Norway.
Explicit consent: an express written statement (not just an affirmative action).

Personal data: any information which identifies a Data Subject, or information relating to a Data Subject who can be identified, directly or indirectly, from that data or from that data and other identifiers in our possession or that we could reasonably access. Personal data do not include anonymised data or data in which the identity of the individual has been irreversibly removed. Personal data can be factual information about an individual (such as a name, email address, location data, or date of birth) or an opinion about an individual's ac-

фактически (например име, имейл адрес, местоположение или дата на раждане) или мнение относно действията или поведението на индивида.

tions or behavior.

Нарушаване на сигурността на Личните данни: всякакво действие или бездействие, което компрометира сигурността, поверителността, целостта или наличността на Личните данни или физическите, технически, административни или организационни мерки за сигурност, които ние или трети лица – доставчици на услуги, сме въвели за защита на данните. Загубата или неупълномощеният достъп, оповестяването или придобиването на Лични данни също представляват Нарушение на сигурността на Личните данни.

Personal data breach: any action or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organizational security that we or third party service providers have implemented to protect data. The loss or unauthorized access, disclosure or acquisition of Personal Data also constitutes a Personal Data Breach.

Уведомления за поверителност: отделни уведомления, които излагат информацията, която може да бъде предоставена на Субектите на данни, когато Компанията събира информация за тях. Тези уведомления могат да приемат формата на общи декларации за поверителност, приложими спрямо конкретна група индивиди (например уведомления за поверителност до служители или политика за поверителност, публикувана на интернет страница) или могат да бъдат самостоятелни, еднократни декларации за поверителност, които се отнасят до Обработка, свързана с конкретна цел.
Обработване: означава всяка операция или съвкупност от операции, извършвана с лични данни или набор от лични данни чрез автоматични или други средства като събиране, записване, организиране, структуриране, съхранение, адаптиране или промяна, извличане, консултиране, употреба, разкриване чрез предаване, разпространяване или друг начин, по който данните стават достъпни, подреждане или комбиниране, ограничаване, изтриване или унищожаване. Обработката също така

Privacy Notices: separate notices setting out information that shall be provided to Data Subjects when the Company collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, privacy notices to employees or a privacy policy published on a website) or they may be stand-alone, one-time privacy statements covering processing related to a specific purpose.
Processing: means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing also includes transmitting or transferring Personal Data to third parties.

включва предаването или трансферирането на Лични данни към трети лица.

Специални категории лични данни (чувствителни лични данни): Лични данни, разкриващи расов или етнически произход, политически възгледи, религиозни или философски убеждения, данни, както и Лични данни, свързани с престъпни деяния и присъди. членство в синдикални организации, данни, свързани с физически или умствени заболявания, сексуалния живот, сексуална ориентация, биометрични или генетични Членове на персонала: всички управители, прокуристи и служители на „Зеебургер - информатик“ ЕООД.

Special categories of personal data (sensitive personal data): personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, physical and mental health data, data concerning a natural person's sex life or sexual orientation, biometric and genetic data, as well as personal data relating to criminal convictions and offences. Staff members: all managers, procurators and employees of Seeburger Informatik EOOD.