ПОЛИТИКА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ НА „ГРУПАМА ЗАСТРАХОВАНЕ“ ЕАД И „ГРУПАМА ЖИВОТОЗАСТРАХОВАНЕ“ ЕАД

I. ВЪВЕДЕНИЕ И ЦЕЛ

Защитата на физическите лица по отношение на обработването на лични данни е основно право, предвидено в Хартата на основните права на Европейския съюз.

Поради разнообразието на дейностите си, Групама Застраховане ЕАД и Групама Животозастраховане ЕАД обработват различни видове лични данни за широк спектър от цели. В контекста на Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните, наричан по-долу „GDPR“), всяко от дружествата действа в качеството на Администратор на лични данни по отношение на извършваните от него дейности.

Съзнавайки важността на защитата на личните данни, Групама Застраховане ЕАД и Групама Животозастраховане ЕАД се стремят да гарантират спазването на основните права и свободи на всички лица – субекти на данни, независимо дали са клиенти, потребители на застрахователни услуги, служители, представители или лица за контакт на партньори и доставчици на услуги. Ние предприемаме всички необходими технически и организационни мерки за защита на Вашата поверителност, в съответствие с високите стандарти и принципи, на които Групата Groupama се подчинява.

В този контекст, настоящата Политика за защита на личните данни има за цел да осигури пълна прозрачност и да Ви предостави ясна информация относно:

- какви са Вашите права като субекти на данни;
- основните принципи и правила, които прилагаме, за да защитим Вашата информация;
- ангажиментите и отговорностите на Групама Застраховане ЕАД и Групама Животозастраховане ЕАД при управлението на Вашите данни.

II. ОБЩИ РАЗПОРЕДБИ

1. *Относими нормативни изисквания*

Политиката отразява изискванията на Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните), който регламент е приложим във всички държави членки на Европейския съюз от 25 май 2018 г. Уредбата за защита на личните данни е доразвита на национално ниво в Закон за защита на личните данни, който регламентира обработването на лични данни на физически лица от администратори и обработващи лични данни на територията на Република България.

PERSONAL DATA PROTECTION POLICY OF "GROUPAMA ZASTRAHOVANE" EAD AND "GROUPAMA ZHIVOTOZASTRAHOVANE" EAD

I. INTRODUCTION AND PURPOSE

The protection of natural persons in relation to the processing of personal data is a fundamental right enshrined in the Charter of Fundamental Rights of the European Union.

Due to the diversity of their activities, Groupama Zastrahovane EAD and Groupama Zhivotozastrahovane EAD process various types of personal data for a wide range of purposes. In the context of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, hereinafter referred to as "GDPR"), each of the companies acts as a Data Controller in relation to the activities it performs.

Recognizing the importance of personal data protection, Groupama Zastrahovane EAD and Groupama Zhivotozastrahovane EAD strive to ensure compliance with the fundamental rights and freedoms of all individuals – data subjects, whether they are clients, users of insurance services, employees, representatives, or contact persons of partners and service providers. We implement all necessary technical and organizational measures to protect your privacy, in accordance with the high standards and principles adhered to by the Groupama Group.

In this context, this Personal Data Protection Policy aims to ensure full transparency and provide you with clear information regarding:

- what your rights as data subjects are;
- the fundamental principles and rules we apply to protect your information;
- the commitments and responsibilities of Groupama Zastrahovane EAD and Groupama Zhivotozastrahovane EAD in the management of your data.

II. GENERAL PROVISIONS

1. *Applicable regulatory requirements*

This Policy reflects the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), which has been applicable in all Member States of the European Union since 25 May 2018. The regulatory framework for personal data protection is further developed at the national level in the Personal Data Protection Act, which regulates the processing of personal data of natural persons by data controllers and data processors within the territory of the Republic of Bulgaria.

2. *Дефиниции*

2.1. Лични данни
Всяка информация, отнасяща се до физическо лице (субект на данни), идентифицирано или възможно да бъде идентифицирано пряко или непряко, като се позовава на идентификационен номер или на един или повече специфични елемента (например фамилия, собствено име, всеки национален идентификационен номер, email адрес, IP адрес, глас, снимка, данни за местоположението и др.).

2.2. Обработване на данни
Всяка операция или набор от операции, включващи лични данни, независимо от използвания метод или средство (автоматизирано обработване на лични данни или неавтоматизирано обработване на лични данни), включително 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 на данни.

2.3. Администратор на лични данни
Физическо или юридическо лице, което е единствено или съвместно отговорно за определяне на целите и средствата за обработване на данни. Всяко едно от дружествата Групама Застраховане ЕАД и Групама Животозастраховане ЕАД е администратор на лични данни и обработва лични данни на своите контрагенти, като в някои случаи обработва личните данни заедно с други администратори на лични данни (съвместни администратори) или чрез обработващи лични данни.

2.4. Обработващ лични данни
Физическо или юридическо лице, което обработва лични данни от името на администратора на лични данни. Всяко едно от дружествата Групама Застраховане АД и Групама Животозастраховане ЕАД е обработващ лични данни от името на другото дружество - администратор на лични данни на базата на договор за споделена ИТ инфраструктура и персонал.

2.5. Орган за защита на личните данни
Национален независим орган, отговорен за надзора на спазването на разпоредбите за защита на личните данни. Комисията за защита на личните данни (КЗЛД) осъществява независимия надзор за спазването на разпоредбите за защита на личните данни в Република България.

2.6. Длъжностно лице по защита на данните
Лице, назначено от администратора на лични данни въз основа на професионална компетентност и познаване на въпросите, свързани със защитата на личните данни, съблюдаващо съответствието при управлението на личните данни с установената нормативна рамка. За Длъжностно лице по защита на личните данни съответно на Групама Застраховане ЕАД и Групама Животозастраховане ЕАД е определен Юрисконсулт – корпоративно управление.

2.7. Отговорник по информационна сигурност
Отговорникът по информационна сигурност на Групама Застраховане ЕАД и Групама Животозастраховане ЕАД (ISO) отговаря за сигурността на информационните системи в рамките на двете дружества. Тази функция се изпълнява от служител от направление Технологии и дигитални операции и представлява ръководна длъжност по смисъла на чл.85 от Кодекса за застраховането.

2. *Definitions*

2.1. Personal Data
Any information relating to a natural person (data subject), identified or identifiable, directly or indirectly, by reference to an identification number or to one or more specific factors (e.g., surname, first name, any national identification number, email address, IP address, voice, photograph, location data, etc.).

2.2. Data Processing
Any operation or set of operations involving personal data, regardless of the method or means used (automated or non-automated processing of personal data), including 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 of data.

2.3. Data Controller
A natural or legal person which is solely or jointly responsible for determining the purposes and means of data processing. Each of the companies Groupama Zastrahovane EAD and Groupama Zhivotozastrahovane EAD is a data controller and processes the personal data of its counterparties, in some cases processing personal data together with other data controllers (joint controllers) or through data processors.

2.4. Data Processor
A natural or legal person which processes personal data on behalf of the data controller. Each of the companies Groupama Zastrahovane AD and Groupama Zhivotozastrahovane EAD acts as a data processor on behalf of the other company - in its capacity as a data controller - based on an agreement for shared IT infrastructure and personnel.

2.5. Data Protection Authority
A national independent authority responsible for supervising compliance with data protection regulations. The Commission for Personal Data Protection (CPDP) carries out independent supervision over compliance with data protection regulations in the Republic of Bulgaria.

2.6. Data Protection Officer
A person appointed by the data controller based on professional competence and knowledge of data protection matters, monitoring compliance in the management of personal data with the established regulatory framework. The Legal Adviser – Corporate Governance is appointed as the Data Protection Officer for Groupama Zastrahovane EAD and Groupama Zhivotozastrahovane EAD, respectively.

2.7. Information Security Officer
The Information Security Officer (ISO) of Groupama Zastrahovane EAD and Groupama Zhivotozastrahovane EAD is responsible for information systems security within the two companies. The role is held by an employee from the Technical and Digital Operations Division and constitutes a managerial position within the meaning of Art. 85 of the Insurance Code.

3. *Принципи*

Общите принципи за защита на личните данни представляват изисквания, които трябва да бъдат изпълнени, преди да се извърши всяко обработване на лични данни, да са налице при самото обработване, както и при всяко следващо изменение на това обработване.

Групама Застраховане ЕАД и Групама Животозастраховане ЕАД и всички техни съвместни администратори на лични данни трябва да бъдат в състояние да демонстрират по всяко време предприетите мерки за спазване на различните изисквания за защита на личните данни.

Принципите на защита на личните данни се вземат предвид от етапа на проектиране на всяко обработване на данни, както и по подразбиране.

3.1. Законосъобразност, добросъвестност и прозрачност
Личните данни се събират добросъвестно, законосъобразно и прозрачно за конкретни, изрични и законни цели и не се обработват повече по начин, който е несъвместим с тези цели. Данните се обработват законосъобразно, когато е налице правно основание за обработването. Основанията за обработване на данните са определени в чл. 6 от GDPR. В по-широк смисъл данните се обработват законосъобразно при прилагане на всички общи принципи.
Данните се събират добросъвестно и прозрачно, когато субектите на данни са информирани за използваното обработване на данни (цели, получатели, периоди на съхранение на данни и т.н.) и за това как те могат да упражнят правата.
Субектите на данни трябва да бъдат информирани по този начин или по времето, когато се събират данни, или в разумен срок в случай на непряко събиране (данни, които не се събират директно от субекта на данните). Разумният срок за уведомяване на субектите на данни в случаите на непряко събиране не може да надхвърля един месец.
За да се осигури, надлежното информиране на субектите на данни дори в случаите по чл.14, параграф 5 (б) от GDPR - когато предоставянето на такава информация се окаже невъзможно или изисква несъразмерно големи усилия, се осигурява публичен достъп до информацията.

3.2. Ограничение на целите
Данните се събират само за конкретни изрично указани и легитимни цели, като не се допуска по-нататъшно обработване по начин, несъвместим с първоначалните цели.

3.3. Свеждане на данните до минимум
Личните данни са подходящи, свързани със и ограничени до необходимото във връзка с целите, за които се обработват (първоначалните и съвместимите последващи цели).

3.4. Точност
Личните данни трябва да бъдат точни и да се поддържат актуални. Трябва да се вземат мерки, за да се гарантира, че личните данни, които са неточни, като се имат предвид целите, за които се обработват, се коригират или заличават незабавно.

3.5. Ограничение за съхранение
Личните данни могат да се съхраняват не повече от необходимото за целите, за които се обработват, в съответствие с приложимото законодателство. Когато вече не е необходимо, те трябва да бъде анонимизирани или унищожени.
Субектите на данни са информирани за периода, за който се съхраняват данните им (или за критериите, позволяващи определянето на периода).

3. *Principles*

The general principles of personal data protection constitute requirements that must be met before any processing of personal data is carried out, shall persist during the processing itself, as well as during any subsequent modification of that processing.

Groupama Zastrahovane EAD and Groupama Zhivotozastrahovane EAD, along with all their joint data controllers, must be able to demonstrate at all times the measures taken to comply with the various data protection requirements.

The principles of data protection shall be taken into account from the design stage of any data processing (privacy by design), as well as by default (privacy by default).

3.1. Lawfulness, Fairness, and Transparency
Personal data shall be collected fairly, lawfully, and transparently for specified, explicit, and legitimate purposes and shall not be further processed in a manner incompatible with those purposes. Data is processed lawfully when there is a legal basis for the processing. The grounds for data processing are defined in Art. 6 of the GDPR. In a broader sense, data is processed lawfully when all general principles are applied.
Data is collected fairly and transparently when data subjects are informed about the data processing used (purposes, recipients, data retention periods, etc.) and how they can exercise their rights.
Data subjects must be informed in this manner either at the time the data is collected or within a reasonable timeframe in case of indirect collection (data not collected directly from the data subject). The reasonable period for notifying data subjects in cases of indirect collection shall not exceed one month.
In order to ensure that data subjects are duly informed, including in the cases referred to in Article 14(5)(b) of the GDPR - where the provision of such information proves impossible or would involve a disproportionate effort - the information shall be made publicly available.

3.2. Purpose Limitation
Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

3.3. Data Minimization
Personal data shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed (the original and compatible subsequent purposes).

3.4. Accuracy
Personal data must be accurate and kept up to date. Measures must be taken to ensure that personal data which is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay.

3.5. Storage Limitation
Personal data may be kept for no longer than is necessary for the purposes for which it is processed, in accordance with applicable legislation. When no longer necessary, data must be anonymized or destroyed.
Data subjects are informed of the period for which their data is stored (or the criteria used to determine that period).

3.6. Цялостност и поверителност
Гарантиране на подходящо ниво на сигурност на личните данни и прилагане на подходящи технически и организационни мерки. Вземат се всички необходими предпазни мерки с оглед на вида данни, обхвата, контекста, целта и рисковете, свързани с обработването и използваните технологии, за да се запази сигурността на данните, включително предотвратяване на повреда, изтриване, обработване за неподходящи цели или достъп до данни от неупълномощени трети страни. Това е задължение на администратора на лични данни и на всички използвани обработващи лични данни впоследствие. Администраторът на лични данни трябва да гарантира, че всеки обработващ данни предлага достатъчни гаранции относно прилагането на подходящи технически и организационни мерки, за да се гарантира, че цялото обработване на данни отговаря на действащите правни и регулаторни изисквания за защита на личните данни. Това задължение следва да бъде формализирано в споразумение, сключено с обработващия данните, като същото не освобождава администратора на лични данни от задължението да гарантира, че мерките са спазени.

3.7. Отчетност
Администраторът на лични данни следва да бъде в състояние на докаже прилагането на принципите пред субекта на данни, както и пред надзорните органи и да носи отговорност за същите.

4. *Основания за обработване на лични данни*

Обработването на лични данни е законосъобразно, ако е налице някое от следните алтернативни и равнопоставени основания:

4.1. Съгласие
За да бъде легитимно, съгласието трябва да отговаря едновременно на всеки един от посочените критерии:
- да е свободно изразено - не е дадено под натиск или заплаха от неблагоприятни последици (напр. по-висока цена на услуга, неравнопоставеност при взаимоотношението с администратора на лични данни);
- да е конкретно - отделно съгласие за всяка конкретно определена цел, а когато е относимо - и за конкретна категория лични данни;
- да е информирано - дадено на основата на пълна, точна и лесно разбираема информация;
- да е недвусмислено – не се извлича или предполага на основата на други изявления или действия на лицето;
- да е изрично изявление или ясно потвърждаващо действие - например с отбелязване на нарочна отметка, чрез натискане на определен бутон и други.

Съгласие не е необходимо и то е невалидно, а изискването му представлява прекомерно обработване на данни, когато данните се обработват въз основа на някое от другите основания.

4.2. Изпълнение на договор
Обработването е законосъобразно, ако:
- е налице договорно правоотношение и обработването на лични данни се осъществява във връзка с изпълнение на договорно задължение;
- са предприети преддоговорни стъпки от страна на субекта на данни (напр. предоставяне на персонализирано предложение за даден продукт/услуга).

4.3. Законово задължение
Общата цел на обработването следва да бъде спазването на правно задължение, което е разписано конкретно в националното законодателство или в правото на Европейския съюз.

3.6. Integrity and Confidentiality
Ensuring an appropriate level of security for personal data and implementing appropriate technical and organizational measures. All necessary precautions are taken, given the type of data, scope, context, purpose, and risks associated with the processing and the technologies used, to preserve data security, including preventing damage, erasure, processing for inappropriate purposes, or access by unauthorized third parties. This is an obligation of the data controller, and all subsequently engaged data processors. The data controller must ensure that each data processor offers sufficient guarantees regarding the implementation of appropriate technical and organizational measures to ensure that all data processing meets the current legal and regulatory requirements for personal data protection. This obligation shall be formalized in an agreement concluded with the data processor, which does not exempt the data controller from the obligation to ensure that the measures are complied with.

3.7. Accountability
The data controller shall be responsible for, and be able to demonstrate compliance with the principles to the data subject as well as to the supervisory authorities.

4. *Legal Grounds for Processing Personal Data*

The processing of personal data is lawful only if at least one of the following alternative and equivalent grounds applies:

4.1. Consent
To be legitimate, consent must simultaneously meet each of the following criteria:
- Freely given - not provided under pressure or threat of adverse consequences (e.g., higher service price, inequality in the relationship with the controller);
- Specific - separate consent for each specifically defined purpose, and where applicable, for a specific category of personal data;
- Informed - provided on the basis of full, accurate, and easily understandable information;
- Unambiguous - not inferred or assumed based on other statements or actions of the individual;
- Explicit statement or clear affirmative action - for example, by ticking a specific checkbox, clicking a certain button, etc.

Consent is not required and is invalid - and requesting it constitutes excessive data processing - when the data is processed based on any of the other legal grounds.

4.2. Performance of a Contract
Processing is lawful if:
- a contractual relationship exists and the processing of personal data is carried out in connection with the performance of a contractual obligation;
- pre-contractual steps have been taken at the request of the data subject (e.g., providing a personalized offer for a specific product/service).

4.3. Legal Obligation
The overall purpose of the processing must be compliance with a legal obligation specifically prescribed in national legislation or European Union law.

4.4. Жизненоважни интереси
Обработването е необходимо, за да бъдат защитени жизненоважните интереси на субекта на данните или на друго физическо лице. Настоящото правно основание е приложимо в най-висока степен за спешната медицинска помощ, в случаите когато трябва да се обработват лични данни за медицински цели, но лицето не е в състояние да даде съгласие за обработването.

4.5. Легитимни интереси
Обработването е необходимо за целите на легитимните интереси на администратора на лични данни или на трета страна, освен когато пред такива интереси преимущество имат интересите или основните права и свободи на субекта на данните, които изискват защита на личните данни

4.6. Обществен интерес/официални правомощия
Обработването е необходимо за изпълнението на задача от обществен интерес или при упражняването на официални правомощия, които са предоставени на администратора на лични данни.

5. *Индивидуални права на субектите на данни*

Всеки субект на данни, чиито данни се обработват, има редица права, които трябва да бъдат спазени от администратора на лични данни, а именно:

5.1. Информираност (чл. 13 и 14 от GDPR)
Правото на кратка, прозрачна, разбираема и лесно достъпна информация за обработването, преди то да се случи, включително идентифициращи данни на администратора, целите и правното основание за обработване, получателите, намерението на администратора лични данни да предаде личните данни на трета страна (когато е приложимо); срок на съхранение на лични данни, информация за всички права, които субектът на данни има, право на жалба до надзорния орган и други.

5.2. Право на достъп (чл. 15 от GDPR)
Субектът на данните има право да получи от администратора на лични данни потвърждение дали се обработват лични данни, свързани с него, и ако това е така, да получи достъп до данните и информацията по чл. 15, параграф 1 и 2 от GDPR, както и да получи копие от личните данни в процес на обработване, което не влияе неблагоприятно върху правата и свободите на други лица.

5.3. Право на коригиране (чл. 16 от GDPR)
Субектът на данни има право да поиска от администратора на лични данни да коригира без ненужно забавяне неточните лични данни, свързани с него. Като се имат предвид целите на обработването субектът на данните има право непълните лични данни да бъдат попълнени.

5.4. Право на изтриване (право „да бъдеш забравен“) (чл. 17 от GDPR)
Субектът на данни може да поиска изтриване, когато личните данни повече не са необходими за целите, за които са били събрани, субектът на данните оттегля своето съгласие, върху което се основава обработването на данните и няма друго правно основание за обработването, личните данни са били обработвани незаконосъобразно и други.

5.5. Право на ограничаване на обработването (чл. 18 от GDPR)
Необходимо е наличието на конкретни условия като:
- Точността на личните данни се оспорва от субекта на данните. В този случай ограничаването на обработването е за срок, който позволява на администратора на лични данни да провери точността на личните данни.

4.4. Vital Interests
Processing is necessary to protect the vital interests of the data subject or another natural person. This legal ground is most applicable to emergency medical care, in cases where personal data must be processed for medical purposes, but the person is unable to provide consent for the processing.

4.5. Legitimate Interests
Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data.

4.6. Public Interest / Official Authority
Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

5. Individual Rights of Data Subjects

Each data subject whose data is being processed has a number of rights that must be respected by the data controller, namely:

5.1. Right to be Informed (Art. 13 and 14 of the GDPR)
The right to concise, transparent, intelligible, and easily accessible information about the processing before it occurs, including the identification data of the data controller, the purposes and legal basis for processing, the recipients, the controller's intention to transfer personal data to a third party (where applicable), the data retention period, information on all rights held by the data subject, the right to lodge a complaint with a supervisory authority, etc.

5.2. Right of Access (Art. 15 of the GDPR)
The data subject has the right to obtain from the controller confirmation as to whether or not personal data concerning them are being processed, and, where that is the case, access to the data and the information under Art. 15, para. 1 and 2 of the GDPR, as well as to receive a copy of the personal data undergoing processing, provided this does not adversely affect the rights and freedoms of others.

5.3. Right to Rectification (Art. 16 of the GDPR)
The data subject has the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning them. Taking into account the purposes of the processing, the data subject has the right to have incomplete personal data completed.

5.4. Right to Erasure (Right to be Forgotten) (Art. 17 of the GDPR)
The data subject may request erasure when the personal data are no longer necessary in relation to the purposes for which they were collected, the data subject withdraws their consent on which the processing is based and there is no other legal ground for the processing, the personal data have been unlawfully processed, etc.

5.5. Right to Restriction of Processing (Art. 18 of the GDPR)
Specific conditions must be met, such as:
- The accuracy of the personal data is contested by the data subject. In this case, the restriction is for a period enabling the controller to verify the accuracy of the personal data.
- The processing is unlawful, but the data subject opposes the erasure of the personal data and requests the restriction of their use instead.

- Обработването е неправомерно, но субектът на данните не желае личните данни да бъдат изтрити, а изисква вместо това ограничаване на използването им.
- Администраторът на лични данни не се нуждае повече от личните данни за целите на обработването, но субектът на данните ги изисква за установяването, упражняването или защитата на правни претенции.
- Субектът на данните е възразил срещу обработването в очакване на проверка дали законните основания на администратора на лични данни имат преимущество пред интересите на субекта на данните.

5.6. Право на преносимост на данните (чл. 20 от GDPR)
Субектът на данните има право да получи личните данни, които го засягат и които той е предоставил на администратор на лични данни, в структуриран, широко използван и пригоден за машинно четене формат и има правото да прехвърли тези данни на друг администратор на лични данни без възпрепятстване от администратора на лични данни, на когото личните данни са предоставени, когато обработването е основано на съгласие или на договорно задължение и обработването се извършва по автоматизиран начин. Когато упражнява правото си на преносимост на данните, субектът на данните има право да получи и пряко прехвърляне на личните данни от един администратор на лични данни към друг, когато това е технически осъществимо.

5.7. Право на възражение (чл. 21 от GDPR)
Администраторът на лични данни е длъжен да прекрати обработването, освен ако не докаже, че съществуват убедителни законови основания, които имат предимство пред интересите, правата и свободите на субекта на данни, или за установяването, упражняването или защитата на правни претенции. При възразяване срещу обработването на лични данни за целите на директния маркетинг, обработването следва да се прекрати незабавно и безусловно.

5.8. Право на субекта на данни да не бъде обект на решение, основаващо се единствено на автоматизирано обработване, включително профилиране (чл. 22 от GDPR)

5.9. Право на защита по съдебен или административен ред, в случай че правата на субекта на данни са били нарушени.

5.10. Правото на обезщетение на всяко лице, което е претърпяло материални или нематериални вреди в резултат на нарушение на горепосочените разпоредби.

Групама Застраховане ЕАД и Групама Животозастраховане ЕАД, съществуват вътрешни процедури за управление на процеса на информиране на субектите на данни и обработване на техните искания в съответствие със законовите и подзаконовите разпоредби.

6. *Специални категории лични данни*

Събирането и обработването на определени категории лични данни са забранени (отнасящи се до расов или етнически произход, политически възгледи, религиозни или философски убеждения, членство в синдикати, генетични или биометрични данни, такива относно здравето или сексуалния живот и сексуалната ориентация и т.н.).

Особено чувствителните данни представляват висок риск по отношение на индивидуалните свободи и основните права. Също така, съществуват ограничения за събирането на данни, свързани с осъдителни присъди и престъпления; други видове данни могат да бъдат ограничени в зависимост от местното законодателство. При много ограничени условия, стриктно определени от регулаторните разпоредби, може да бъде възможно да се премахне общата забрана за обработване на такива данни (изрично съгласие,

- The controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise, or defense of legal claims.
- The data subject has objected to processing pending the verification whether the legitimate grounds of the controller override those of the data subject.

5.6. Right to Data Portability (Art. 20 of the GDPR)
The data subject has the right to receive the personal data concerning them, which they have provided to a controller, in a structured, commonly used, and machine-readable format and has the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where the processing is based on consent or a contract and the processing is carried out by automated means. When exercising the right to data portability, the data subject has the right to have the personal data transmitted directly from one controller to another, where technically feasible.

5.7. Right to Object (Art. 21 of the GDPR)
The data controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights, and freedoms of the data subject, or for the establishment, exercise, or defense of legal claims. Where personal data are processed for direct marketing purposes, the processing shall be discontinued immediately and unconditionally.

5.8. Right of the data subject not to be subject to a decision based solely on automated processing, including profiling (Art. 22 of the GDPR)

5.9. Right to judicial or administrative redress in case the data subject's rights have been violated.

5.10. Right to compensation for any person who has suffered material or non-material damage as a result of an infringement of the aforementioned provisions.

Groupama Zastrahovane EAD and Groupama Zhivotozastrahovane EAD have established internal procedures for managing the process of informing data subjects and processing their requests in accordance with statutory and regulatory provisions.

6. *Special Categories of Personal Data/ Sensitive Data*

The collection and processing of certain categories of personal data are prohibited (referring to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic or biometric data, data concerning health or a person's sex life and sexual orientation, etc.).

Particularly sensitive data represent a high risk to individual freedoms and fundamental rights. Furthermore, there are restrictions on the collection of data related to criminal convictions and offences; other types of data may be restricted depending on local legislation. Under very limited conditions, strictly defined by regulatory provisions, it may be possible to lift the general prohibition on processing such data (explicit consent, establishment, exercise, or defense of legal claims, public

установяване, упражняване или защита на правни претенции, обществен интерес и т.н.). В Кодекса за застраховането има предвидени законови основания за обработване на чувствителни лични данни в ограничени случаи.

Групама Застраховане ЕАД и Групама Животозастраховане ЕАД следят приложимото законодателството за защита на личните данни, за да гарантират съответствие, като се обръща специално внимание на тези категории данни.

7. *Прехвърляне на данни в страни извън ЕС*

Групама Застраховане ЕАД и Групама Животозастраховане ЕАД са базирани в страна от Европейския съюз и следователно гарантират, че прехвърлянето на данни в държава, която не е член на Европейския съюз, е възможно само ако тази държава осигурява адекватно ниво на защита, или ако са налице подходящи правни гаранции или ако прехвърлянето попада в приложното поле на дерогациите, разрешени от регламентите.

Когато администраторът на лични данни използва обработващ лични данни, администраторът на лични данни трябва да провери дали данните се прехвърлят в страна извън Европейския съюз от обработващия на данни или от каквито и да е подизпълнители на обработващи на лични данни, които самият обработващ може да използва, и контролира тези трансфери в зависимост от държавата на направлението.

III. НАРУШЕНИЯ НА СИГУРНОСТТА НА ЛИЧНИТЕ ДАННИ

Нарушение на сигурността на личните данни е всяко нарушение на сигурността, което води до случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или достъп до лични данни, които се предават, съхраняват или обработват по друг начин.

В случай на нарушение на сигурността на личните данни администраторът на лични данни, без ненужно забавяне и когато това е осъществимо - не по-късно от 72 часа след като е разбрал за него, уведомява за нарушението на сигурността на личните данни надзорния орган за защита на личните данни, освен ако не съществува вероятност нарушението на сигурността на личните данни да породи риск за правата и свободите на физическите лица.

Обработващият лични данни уведомява администратора на лични данни без ненужно забавяне, след като узнае за нарушаване на сигурността на лични данни.

Когато има вероятност нарушението на сигурността на личните данни да породи висок риск за правата и свободите на физическите лица, администраторът на лични данни, без ненужно забавяне, съобщава на субекта на данните за нарушението на сигурността на личните данни. Същото не се изисква, ако:

- администраторът на лични данни е предприел подходящи технически и организационни мерки за защита и тези мерки са били приложени по отношение на личните данни, засегнати от нарушението на сигурността на личните данни, по-специално мерките, които правят личните данни неразбираеми за всяко лице, което няма разрешение за достъп до тях, като например криптиране;
- администраторът на лични данни е взел впоследствие мерки, които гарантират, че вече няма вероятност да се материализира високият риск за правата и свободите на субектите на данни;
- то би довело до непропорционални усилия; в такъв случай се прави публично съобщение или се взема друга

interest, etc.). The Insurance Code provides legal grounds for the processing of sensitive personal data in limited cases.

Groupama Zastrahovane EAD and Groupama Zhivotozastrahovane EAD monitor the applicable data protection legislation applicable to ensure compliance, with special attention paid to these categories of data.

7. *Data Transfers to Countries Outside the European Union*

Groupama Zastrahovane EAD and Groupama Zhivotozastrahovane EAD are based in an European Union Member State and, therefore, ensure that the transfer of data to a country that is not a member of the European Union is only possible if that country provides an adequate level of protection, or if appropriate legal safeguards are in place, or if the transfer falls within the scope of the derogations permitted by the regulations.

When the data controller engages a data processor, the data controller must verify whether data is being transferred to a country outside the European Union by the data processor or by any sub-processors that the processor itself may use, and must control these transfers depending on the country of destination.

III. PERSONAL DATA BREACHES

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed.

In the case of a personal data breach, the data controller shall, without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

The data processor shall notify the data controller without undue delay after becoming aware of a personal data breach.

When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the data controller shall communicate the personal data breach to the data subject without undue delay. Such communication shall not be required if:

- the data controller has implemented appropriate technical and organizational protection measures, and those measures were applied to the personal data affected by the breach, in particular those that render the personal data unintelligible to any person who is not authorized to access it, such as encryption;
- the data controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialize;
- it would involve disproportionate effort; in such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

подобна мярка, така че субектите на данни да бъдат в еднаква степен ефективно информирани.

Всяко от дружествата Групама Застраховане ЕАД и Групама Животозастраховане ЕАД като администратори на лични данни е отговорно за управлението на нарушенията на сигурността на личните данни и за уведомяването на надзорния орган за защита на личните данни и на субектите на данни, като за целта:

- осигурява способност за своевременно установяване и докладване на нарушения на сигурността на личните данни;
- гарантира, че в договореностите с Обработващите лични данни са предвидени клаузи, предвиждащи задължения за уведомяване при нарушение на сигурността на лични данни в определен за това срок, както и предприемане на необходимите стъпки, с цел намаляване на неблагоприятните последици, поправяне на нарушението на сигурността и избягване на бъдещи нарушения;
- документира обстоятелствата, свързани с всяко нарушение на сигурността на личните данни, техните последици и всички предприети мерки за тяхното отстраняване; тази документация следва да бъде съхранявана надлежно;
- ако е необходимо, преразглежда своите оценки на въздействието върху защитата на данните с цел намаляване на риска от нарушения на сигурността.

IV. ОСВЕДОМЕНОСТ

Всички служители на Групама Застраховане ЕАД и Групама Животозастраховане ЕАД се обучават в съответствие с актуалната нормативна рамка, уреждаща защитата на личните данни. Повишаването на осведомеността и обучението допринасят за намаляване на рисковете, когато се идентифицира човешкият фактор като потенциален риск (грешки, небрежност, отклонено поведение) и действа като средство за защита на личните данни (придобиване на навик на бдителност и способност да се реагира при нарушения).

Подробна информация относно конкретните категории лични данни, които събираме, целите на обработване, получателите и сроковете за съхранение, специфични за съответното правоотношение, ще откриете в Уведомления за поверителност, достъпни на нашия уебсайт: www.groupama.bg.

Each of the companies Groupama Zastrahovane EAD and Groupama Zhivotozastrahovane EAD, as data controllers, is responsible for managing personal data breaches and for notifying the supervisory authority and the data subjects, and in this respect:

- ensures the capability to identify and report personal data breaches in a timely manner;
- ensures that agreements with Data Processors include clauses stipulating notification obligations within a specified timeframe, as well as taking necessary steps to mitigate adverse effects, remediate the breach, and prevent future occurrences;
- document the circumstances relating to each personal data breach, its effects, and any remedial action taken; this documentation must be properly stored;
- if necessary, reviews its data protection impact assessments (DPIA) to mitigate the risk of security breaches.

IV. AWARENESS

All employees of Groupama Zastrahovane EAD, and Groupama Zhivotozastrahovane EAD are trained in accordance with the current regulatory framework governing personal data protection. Awareness-raising and training contributes to risk reduction where the human factor is identified as a potential risk (errors, negligence, deviant behaviour) and act as a means of personal data protection (developing a habit of vigilance and the ability to react to breaches).

Detailed information regarding the specific categories of personal data we collect, the purposes of processing, the recipients, and the retention periods specific to the respective legal relationship, can be found in the Privacy Notices available on our website: www.groupama.bg.