ИМАЙКИ ПРЕДВИД, ЧЕ:

„ЛИЧНИ ДАННИ” означава всяка информация, отнасяща се до физическо лице, което е идентифицирано или може да бъде идентифицирано пряко или непряко чрез идентификатор като име, идентификационен номер, данни за местонахождение, онлайн идентификатор или чрез един или повече специфични признаци – признаци, свързани с физическа, физиологична, генетична, психическа, умствена, икономическа, културна, социална или друга идентичност на това физическо лице.

„ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ” 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.

„РЕГИСТЪР С ЛИЧНИ ДАННИ“ означава всеки структуриран набор от лични данни, достъпът до които се осъществява съгласно определени критерии, независимо дали е централизиран, децентрализиран или разпределен съгласно функционален или географски принцип.

„АДМИНИСТРАТОР“ означава 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.

ИМАЙКИ ПРЕДВИД, ЧЕ:

Задължение на АДМИНИСТРАТОРА е да осигури спазването на принципите за обработване на лични данни и по-конкретно да:

* се обработват законосъобразно и добросъвестно;

* бъдат съотносими, свързани със и ненадхвърлящи целите, за които се обработват;
* бъдат точни и при необходимост да се актуализират;
* се заличават или коригират, когато се установи, че са неточни или непропорционални по отношение на целите, за които се обработват;
* се поддържат във вид, който позволява идентифициране на съответните физически лица за период не по-дълъг от необходимия за целите, за които тези данни се обработват;

ФОНДАЦИЯ „КЕРА“, в качеството си на **АДМИНИСТРАТОР НА ЛИЧНИ ДАННИ приема настоящия ПРАВИЛНИК ЗА ОПРЕДЕЛЯНЕ НА ТЕХНИЧЕСКИ И ОРГАНИЗАЦИОННИ МЕРКИ И ВИДОВЕТЕ ЗАЩИТА НА ЛИЧНИТЕ ДАННИ ВЪВ**

ФОНДАЦИЯ „КЕРА” с цел да определи принципите, основанията, техническите и организационни мерки при обработване на лични данни и допустимия вид защита в съответствие със законодателството на ЕС (Общия регламент за защита на данните (Регламент (ЕС) 2016/679)) и на Република България (Закона за защита на личните данни, на подзаконовите нормативните актове по прилагането му) по отношение на обработването на личните данни и защитата на правата и свободите на лицата, чиито лични данни **ФОНДАЦИЯ „КЕРА”** събира и обработва.

ПРАВИЛНИК
ЗА ОПРЕДЕЛЯНЕ НА ТЕХНИЧЕСКИ И ОРГАНИЗАЦИОННИ МЕРКИ И ВИДОВЕТЕ ЗАЩИТА НА ЛИЧНИТЕ ДАННИ ВЪВ ФОНДАЦИЯ „КЕРА”

ОБЩИ ПОЛОЖЕНИЯ

Чл. 1. (1) С този правилник се определят принципите, основанията, техническите и организационни мерки при обработване на лични данни и допустимия вид защита в съответствие със законодателството на ЕС (Общия регламент за защита на данните (Регламент (ЕС) 2016/679)) и на Република България (Закона за защита на личните данни, на подзаконовите нормативните актове по прилагането му) по отношение на обработването на личните данни и защитата на правата и свободите на лицата, чиито лични данни **ФОНДАЦИЯ „КЕРА”** събира и обработва.

(2) Този правилник се отнася до всички функции по обработването на лични данни, включително лични данни на работници/служители, туристи(клиенти) – възложители по договор за туристическа услуга, доставчици, партньори и всякакви други лични данни, които организацията обработва от различни източници.

(3) Този правилник се прилага и е задължителен за всички учредители/служители и други заинтересовани страни на **ФОНДАЦИЯ „КЕРА”** като външни доставчици и клиенти. Всяко нарушение на Общия регламент за защита на данните (Регламент (ЕС) 2016/679), на Закона за защита на личните данни, на

подзаконовите нормативни актове по прилагането му, както и на настоящия правилник от страна на учредителите и служителите ще бъде разглеждано като нарушение на трудовата дисциплина.

(4) Партньори и трети лица, които работят с или за **ФОНДАЦИЯ „КЕРА”**, както и които имат или могат да имат достъп до лични данни, предоставени им или известни им от **ФОНДАЦИЯ „КЕРА”** следва да се запознаят, разбират и да се съобразят с настоящите правила. Никоя трета страна не може да има достъп до лични данни, съхранявани от **ФОНДАЦИЯ „КЕРА”**, без предварително да е сключила споразумение за поверителност на данните и което дава право на **ФОНДАЦИЯ „КЕРА”** да проверява спазването на приетите със споразумението задължения.

ПРИНЦИПИ НА ОБРАБОТВАНЕТО

Чл. 2. (1) ФОНДАЦИЯ „КЕРА” обработва лични данни при спазване на следните принципи:

а) законосъобразно, добросъвестно и по прозрачен начин по отношение на субекта на данните (принцип на законосъобразност, добросъвестност и прозрачност);

б) лични данни във ФОНДАЦИЯ „КЕРА” се събират само за конкретни, изрично указани и легитимни цели и не се обработват по-нататък по начин, несъвместим с тези цели (принцип на ограничение на целите);

в) личните данни във ФОНДАЦИЯ „КЕРА” са подходящи, свързани с и ограничени до необходимото във връзка с целите, за които се обработват (принцип на свеждане на данните до минимум);

г) личните данни във ФОНДАЦИЯ „КЕРА” следва да бъдат винаги точни и да се поддържат в актуален вид. Неточни лични данни се изтриват или коригират в най-кратки срокове (принцип на точност);

д) Личните данни във ФОНДАЦИЯ „КЕРА” се съхраняват във форма, която да позволява идентифицирането на субекта на данните за период, не по-дълъг от необходимото за целите, за които се обработват личните данни (принцип на ограничение на съхранението);

е) Личните данни във ФОНДАЦИЯ „КЕРА” се обработват по начин, който гарантира подходящо ниво на сигурност, включително защита срещу неразрешено или незаконосъобразно обработване и срещу случайна загуба, унищожаване или повреждане, като се прилагат подходящи технически или организационни мерки (принцип на цялостност и поверителност);

(2) ФОНДАЦИЯ „КЕРА” следи за стриктното спазване на тези принципи и предприема описаните по – долу мерки, за да може във всеки един момент да удостовери спазването им.

ОСНОВАНИЯ ЗА ОБРАБОТВАНЕТО

Чл. 3. (1) ФОНДАЦИЯ „КЕРА” обработва лични данни само, ако е налице поне едно от следните условия (основания):

а) субектът на данните е дал съгласие за обработване на личните му данни, при спазване на условията за даване на съгласие, посочени по-долу в чл. 4;

б) обработването е необходимо за изпълнението на договор, по който субектът на данните е страна, или за предприемане на стъпки по искане на субекта на данните преди сключването на договор;

в) обработването е необходимо за спазването на законово задължение, което се прилага спрямо **ФОНДАЦИЯ „КЕРА”**;

г) обработването е необходимо, за да бъдат защитени жизненоважните интереси на субекта на данните или на друго физическо лице;

д) обработването е необходимо за изпълнението на задача от обществен интерес;

е) обработването е необходимо за целите на легитимните интереси на

ФОНДАЦИЯ „КЕРА” или на трета страна, освен когато пред такива интереси преимущество имат интересите или основните права и свободи на субекта на данните. Първоначалната преценка относно кои интереси имат преимущество е на **ФОНДАЦИЯ „КЕРА”** като в случай на колебание, управителят на **ФОНДАЦИЯ „КЕРА”** може да се обърне към Комисията за защита на личните данни.

(2) **ФОНДАЦИЯ „КЕРА”** обработва специални категории лични данни по смисъла на чл. 9 от Регламент (ЕС) 2016/679, както и данни, свързани с присъди и нарушения по смисъла на чл. 10 от Регламент (ЕС) 2016/679 по изключение и само в случаите, когато такива се изискват по закон, напр. при постъпване на работа на нови служители.

(3) За всяка дейност по обработване на лични данни е необходимо да е налице едно от горепосочените основания. Забранява се обработване на лични данни за други цели, различни от тези, за които първоначално са били събрани, освен ако на отделно основание не е налице някое от посочените по-горе условия в ал.1.

чл. 4. (1) Когато обработването се извършва въз основа на съгласие, **ФОНДАЦИЯ „КЕРА”** отправя искането към субекта на лични данни за съгласието му в разбираема и лесно достъпна форма и използва ясен и прост език.

(2) Като „съгласие“ **ФОНДАЦИЯ „КЕРА”** ще приема всяко свободно изразено, конкретно, информирано и недвусмислено указание за волята на субекта на данните, посредством изявление или ясно потвърждаващо действие, което изразява съгласието му свързаните с него лични данни да бъдат обработени.

(3) ФОНДАЦИЯ „КЕРА” приема за "съгласие" само случаите, в които субектът на данните е бил напълно информиран за планираното обработване и е изразил своето съгласие и 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.

(4) Съгласието не може да бъде изведено от липсата на отговор на съобщение до субекта на данни.

(5) В повечето случаи съгласието за обработка на лични данни се получава рутинно от **ФОНДАЦИЯ „КЕРА”** като се използват стандартни документи за

съгласие.

(6) ФОНДАЦИЯ „КЕРА” информира субекта на данни, че може да оттегли съгласието си по всяко време и без да е необходимо да обосновава причина за оттеглянето. **ФОНДАЦИЯ „КЕРА”** информира субекта на данните, че оттеглянето на съгласието не засяга законосъобразността на обработването, основано на съгласието му, дадено преди неговото оттегляне. **ФОНДАЦИЯ „КЕРА”** предоставя и-мейл адрес и пощенски адрес, на който субектите на данните могат да отправят своите запитвания и да оттеглят съгласието си.

КАТЕГОРИИ ЛИЧНИ ДАННИ И ЦЕЛИ НА ОБРАБОТВАНЕТО

Чл. 5. (1) ФОНДАЦИЯ „КЕРА” определя следните категории лични данни, които ще обработва:

1.1. Данни на членове и управителните органи на фондацията– имена, данни по лична карта.

Цел, за която се събират данните – във връзка с изпълнение на правата и задълженията на членовете, описани в устава.

Основание за обработка на тези лични данни – участието/заявяването на участие като член на **ФОНДАЦИЯ „КЕРА”** и съгласие с нейния устав.

1.2. Данни за връзка с членовете на фондацията - имена, телефон, имейл, адрес.

Цел, за която се събират данните - Осъществяване на връзка с тях, поддържане на контакт и изпращане на информация;

Основание за обработка на тези лични данни – изрично получено съгласие.

2. Данни на трети външни лица, с които **ФОНДАЦИЯ „КЕРА”** сключва договор за изпълнение на отделни негови цели и дейности- имена, ЕГН, данни по документ за самоличност, адрес, имейл, телефон.

Цел, за която се събират данните – във връзка с изпълнение на дейностите, възложени по договор между дружеството и третите лица, осъществаване на контакт с тях при необходимост.

Основание за обработка на тези лични данни - изпълнение на договорно

задължение.

(2) Когато обработването се извършва въз основа на съгласие, за обработването на лични данни на деца под 16 години **ФОНДАЦИЯ „КЕРА”** изисква съгласието да е дадено или разрешено от носещия родителска отговорност за детето. При липса на такова съгласие, обработване не се осъществява, а евентуално получените лични дании се унищожават.

Чл. 6. Обработването на посочените в чл. 5 категории лични данни се осъществява с оглед посочените в същия член цели.

ВИДОВЕ ЗАЩИТА

Чл. 7. ФОНДАЦИЯ „КЕРА” определя следните видовете защита на личните данни в рамките на организацията: физическа, персонална, документална, защита на автоматизирани информационни системи и/или мрежи и криптографска защита.

Чл. 8. (1) Физическата защита на личните данни представлява система от технически и организационни мерки за предотвратяване на нерегламентиран достъп до сградата, помещенията и съоръженията, в които се съхраняват и обработват личните данни.

(2) В помещенията на Администратора е изградена система за контрол на достъпа – обектът се заключва.

ФОНДАЦИЯ „КЕРА” прилага и следи за изпълнението на следните организационни мерки на физическата защита:

1. помещенията, в които се обработват лични данни във **ФОНДАЦИЯ „КЕРА”** са: офис;

2. помещенията, в които ще се разполагат елементите на комуникационно-информационните системи за обработване на лични данни във **ФОНДАЦИЯ „КЕРА”** са: офис;

3. организацията на физическия достъп във **ФОНДАЦИЯ „КЕРА”** е: Външни посетители се допускат само от член на управителните органи на **ФОНДАЦИЯ „КЕРА”**

4. режима на посещения във **ФОНДАЦИЯ „КЕРА”** е: в рамките на работното време, след предварителна уговорка и задължително посетителите се посрещат от член на управителните органи на **ФОНДАЦИЯ „КЕРА”**

5. екип за реагиране при нарушения във **ФОНДАЦИЯ „КЕРА”** се състои от:

Председател на **ФОНДАЦИЯ „КЕРА”** или назначено от него лице.

(3) Основните технически мерки на физическата защита са:

1. ключалки;
2. шкафове;
3. оборудване на зоните с контролиран достъп;
4. оборудване на помещенията;
5. устройства за контрол на физическия достъп;
6. охрана и/или система за сигурност;
7. пожарогасителни средства;

Чл. 9. (1) Персоналната защита представлява система от организационни мерки спрямо физическите лица, които обработват лични данни по указание на **ФОНДАЦИЯ „КЕРА”.**

(2) "ФОНДАЦИЯ „КЕРА” прилага и следи за изпълнението на следните мерки на персоналната защита:

1. познаване на нормативната уредба в областта на защитата на личните данни - запознаване с разпоредбите на РЕГЛАМЕНТ (ЕС) 2016/679 НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА от 27 април 2016 година относно защитата на физическите лица (Общ регламент относно защитата на данните), на Закона за защита на личните данни(ЗЗЛД) и неговите най–актуални изменения и допълнения, на приетите във връзка с ЗЗЛД Наредби, правилници на Комисията за защита на личните данни и нейните актуални становища;

2. познаване на политиката и ръководствата за защита на личните данни - запознаване с настоящите правила и политиката на **ФОНДАЦИЯ „КЕРА”**, с принципите и основанията за законосъобразно обработване на данните, задължението

на физическите лица, които обработват лични данни по указание на **ФОНДАЦИЯ „КЕРА”**, да докладват относно изпълнението на мерките по защита на личните данни на управителя, както и в случай на нарушение на сигурността на лични данни;

3. знания за опасностите за личните данни - разясняване на случаите, при които е налице опасност от нарушение на сигурността на лични данни, минимализиране на рисковите дейности, предварително съгласуване с управителя при необходимост от предприемането на такива действия;

4. споделяне на секретна информация между персонала (например пароли за достъп и др.) - забрана за споделяне на индивидуални пароли за достъп до база с лични данни, смяна на пароли за достъп до такива данни на всеки 3 месеца, при напускане на служител/работник, който е притежавал такава парола, същата се заменя с нова веднага.

5. съгласие за поемане на задължение за неразпространение на личните данни - всички служители/работници и въобще лица, които обработват лични данни по указание на **ФОНДАЦИЯ „КЕРА”**, декларират писмено, че са съгласни и поемат задължението да не разпространяват личните данни, станали им известни при и/или по повод на тяхната работа, при нарушение на това задължение подлежат на дисциплинарна отговорност в рамките на организацията; публичен достъп до ЕГН/ЛНЧ се предоставя, само ако закон изисква това. В тези случаи законът определя реда и условията за достъп с цел недопускане неговата общодостъпност.

6. обучение – еднократно - при постъване на работа/предаване на достъп до лични данни и периодично на всеки 6 месеца;

7. тренировка/ инструктаж на персонала за реакция при събития, застрашаващи сигурността на данните.

(3) Мерките за персонална защита целят предоставяне на достъп до лични данни само на лица, чиито служебни задължения или конкретно възложена задача изискват такъв достъп, при спазване на принципа свеждане на данните до минимум.

(4) Лицата могат да започнат да обработват лични данни след запознаване със:

1. нормативната уредба в областта на защитата на личните данни;

2. политиката и ръководствата за защита на личните данни;

3. опасностите за личните данни.

(5) Обработването на лични данни "извън офиса" представлява потенциално по-голям риск от загуба, кражба или нарушение на лични данни. Персоналът следва да бъде специално упълномощен да обработва данните извън обектите на **ФОНДАЦИЯ „КЕРА“**

(6) Лицата подписват декларация за неразгласяване на лични данни, до които са получили достъп при и по повод изпълнение на задълженията си.

(7) ФОНДАЦИЯ „КЕРА” поддържа и събира информация за изпълнение на задълженията си по настоящия член.

Чл. 10. (1) Документалната защита представлява система от организационни мерки при обработването на лични данни на хартиен носител.

(2) ФОНДАЦИЯ „КЕРА” прилага и следи за изпълнението на следните мерки на документалната защита:

1. Записите с лични данни 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.

2. Записите с лични данни върху хартиен носител се обработват само при наличие на основанията, посочени в чл. 3 и с оглед конкретните цели посочени в чл. 6 от настоящите правила;

3. регламентиране на достъпа до записите с лични данни върху хартиен носител - достъп до регистрите ще има Управителя и/или назначено от него лице;

4. контрол на достъпа до записите с лични данни върху хартиен носител - осъществява се от представител на Управителния съвет;

5. срок за съхранение на записите с лични данни върху хартиен носител - за следните категории записи се съблюдават нормативнопредвидените срокове за съхранение:

- ведомости за заплати и документи, удостоверяващи трудов стаж – 50 години;

- счетоводни и финансови отчети – 10 години;

- фактури, договори и всички документи, касаещи данъчно-осигурителен контрол – 5 години след изтичането на давностния срок за погасяване на публичното задължение, с което са свързани;

- всички останали носители – 5 години.

След изтичането на срока за съхранението, носителите на информация, които не подлежат на предаване в Националния архивен фонд, могат да се унищожат.

6. правила за размножаване и разпространение на записите с лични данни върху хартиен носител - забранява се размножаването и разпространението на записите освен по изрично нареждане на управителя;

7. процедура за унищожаване - след изтичането на срока за съхранение и ако не е налице друго законово основание за съхранение, информацията се унищожава под ръководството на управителя, за което се съставя протокол;

8. проверка и контрол на обработването на записите с лични данни - осъществяват се от управителя;

(3) При сключване на трудов договор са необходими:

1. документ за самоличност, който се връща веднага;
2. документ за придобито образование, специалност, квалификация, правоспособност, когато такива се изискват за длъжността или работата, за която лицето кандидатства;
3. документ за стаж по специалността, когато за длъжността или работата, за която лицето кандидатства, се изисква притежаването на такъв трудов стаж;
4. документ за медицински преглед при първоначално постъпване на работа и след преустановяване на трудовата дейност по трудово правоотношение за срок над 3 месеца;
5. свидетелство за съдимост, когато такова се изисква за съответната длъжност;
6. разрешение от инспекцията по труда, ако лицето не е навършило 16 години или е на възраст от 16 до 18 години.
7. Работодателят може да изисква представянето и на други документи извън посочените ако това е предвидено или произтича от закон или друг нормативен акт.
8. Документ за самоличност, свидетелство за управление на моторно превозно средство, документ за пребиваване на работник/ служител, могат да се копират от работодателя, само ако това е предвидено или произтича от закон или друг нормативен акт.

9. Работодателят съхранява горецитираните документи в лично трудово досие на всеки работник, заедно с:

- трудов договор и допълнителни споразумения;
- молба за назначаване и декларация-съгласие за обработване на лични данни;
- заверено уведомление по чл. 62, ал. 5 от КТ;
- длъжностна характеристика;
- декларация по Наредба № 5 от 20.02.1987г. за болестите, при които работниците, боледуващи от тях, имат особена закрила, съгласно чл. 333, ал.1 от Кодекса на труда;
- декларации по чл. 348, ал. 3 от КТ за трудовата книжка и съхраняване на копие от нея;
- служебна бележка за проведен инструктаж по ЗЗБУТ;
- молби и заповеди за отпуски;
- други – според индивидуалния характер на трудовото правоотношение.

(4) При сключване на граждански договор са необходими:

документ за самоличност, който се връща веднага;

1. документ за придобито образование, специалност, квалификация, правоспособност, когато такива се изискват за длъжността или работата, за която лицето кандидатства;
2. документ за стаж по специалността, когато за длъжността или работата, за която лицето кандидатства, се изисква притежаването на такъв стаж;
3. Администраторът може да изисква представянето и на други документи извън посочените ако това е предвидено или произтича от закон или друг нормативен акт.
4. Документ за самоличност, свидетелство за управление на моторно превозно средство, документ за пребиваване в страната, могат да се копират от администратора, само ако това е предвидено или произтича от закон или друг нормативен акт.

(5) В процедури по подбор на персонал, срокът за съхранение на лични данни на участници в процедурата, не може да бъде по-дълъг от 3 месеца. Когато в процедура

по подбор са изискани да се представят оригинали или нотариално заверени копия на документи, удостоверяващи физическа и психическа годност на кандидата, необходимата квалификационна степен и стаж за заеманата длъжност, субектът на данните, който не е одобрен за назначаване, може да поиска в 30-дневен срок от окончателното приключване на процедурата по подбор да получи обратно представените документи. В тези случаи документите се връщат, по начина, по който са подадени.

(6) След прекратяване на трудовото правоотношение, работодателят съхранява екземпляр от трудов договор, допълнителни споразумения, ведомости за заплати, копие от трудовата книжка, молби и заповеди за отпуск и всички други документи, удостоверяващи трудов стаж за срок от 50 години.

Чл. 11. (1) Защита на автоматизираните информационни системи и/или мрежи представлява система от технически и организационни мерки за защита от незаконни форми на обработване на личните данни. По отношение на автоматизираното обработване на лични данни, след оценка на рисковете се прилагат такива мерки, които имат за цел:

1. контрол върху достъпа до оборудване - да се откаже достъп на неоправомощени лица до оборудването, използвано за обработване;
2. контрол върху носителите на данни - да се предотврати четенето, копирането, изменянето или отстраняването на носители на данни от неоправомощени лица;
3. контрол върху съхраняването - да се предотврати въвеждането на лични данни от неоправомощени лица, както и извършването на проверки, изменянето или заличаването на съхранявани лични данни от неоправомощени лица;
4. контрол върху потребителите - да се предотврати използването на автоматизирани системи за обработване от неоправомощени лица чрез използване на оборудване за предаване на данни;
5. контрол върху достъпа до данни - да се гарантира, че лицата, на които е разрешено да използват автоматизирана система за обработване, имат достъп само до личните данни, които са обхванати от тяхното разрешение за достъп;

6. контрол върху комуникацията - да се гарантира възможността за проверка и установяване на кои органи са били или могат да бъдат предадени или имат достъп до лични данни чрез оборудване за предаване на данни;

7. контрол върху въвеждането на данни - да се гарантира възможността за последваща проверка и установяване на това какви лични данни са били въведени в автоматизираните системи за обработване, както и кога и от кого са били въведени тези лични данни;

8. контрол върху пренасянето - да се предотврати четенето, копирането, изменянето или заличаването на лични данни от неоправомощени лица при предаването на лични данни или при пренасянето на носители на данни;

9. възстановяване - да се гарантира възможността за възстановяване на инсталираните системи в случай на отказ на функциите на системите;

10. надеждност - да се гарантира изпълнението на функциите на системата и докладването за появили се във функциите дефекти;

11. цялостност - да се гарантира недопускане на увреждане на съхраняваните лични данни вследствие на неправилно функциониране на системата.

(2) ФОНДАЦИЯ „КЕРА” прилага и следи за изпълнението на следните мерки за защита на автоматизираните информационни системи и/или мрежи са:

1. политика за защита на личните данни, ръководства по защита и стандартни операционни процедури; в системите за автоматизирано обработване следва да се водят записи (логове) най-малко за следните операции по обработване: събиране, промяна, справки, разкриване, включително предаване, комбиниране и изтриване; записите за извършена справка или разкриване трябва да дават възможност за установяване на основанието, датата и часа на такива операции и доколкото е възможно - идентификацията на лицето, което е направило справка или е разкрило лични данни, както и данни, идентифициращи получателите на тези лични данни; записите се използват единствено за проверяване на законосъобразността на обработването, за самоконтрол, за гарантиране на цялостността и сигурността на личните данни и при наказателни производства; Администраторът определя подходящи срокове за съхранение, вкл. архивиране на записите.

2. определяне на роли и отговорности;

3. идентификация и автентификация, псевдоминимизация; публичен достъп до ЕГН/ЛНЧ се предоставя, само ако закон изисква това; в случай на предоставяне на услуги по електронен път, да се предприемат подходящи технически и организационни мерки, които не позволяват единният граждански номер да е единственият идентификатор за предоставяне на съответната услуга;

4. управление на регистрите;

5. контроли на сесията;

6. външни връзки/свързване;

7. телекомуникации и отдалечен достъп;

8. наблюдение;

9. защита от вируси;

10. планиране на случайността/непредвидените случаи;

11. поддържане/експлоатация;

12. управление на конфигурацията;

13. копия/резервни копия за възстановяване;

14. носители на информация;

15. физическа среда/обкръжение - компютърните екрани и терминалите не могат да бъдат гледани от друг, освен от оторизираните служители / работници на компанията.

16. персонална защита;

17. тренировка на персонала за реакция при събития, застрашаващи сигурността на данните;

18. определяне на срокове за съхранение на личните данни;

19. процедури за унищожаване/заличаване/изтриване на носители.

Чл. 12. (1) Криптографската защита представлява система от технически и организационни мерки, които се прилагат с цел защита на личните данни от нерегламентиран достъп при предаване, разпространяване или предоставяне.

(2) ФОНДАЦИЯ „КЕРА” прилага и следи за изпълнението на следните мерки на криптографската защита:

1. стандартните криптографски възможности на операционните системи;

2. стандартните криптографски възможности на системите за управление на бази данни;

3. стандартните криптографски възможности на комуникационното оборудване;

4. системи за разпределение и управление на криптографските ключове;

5. нормативно определените системи за електронен подпис.

РЕГИСТЪР НА ДЕЙНОСТИТЕ ПО ОБРАБОТВАНЕ

Чл. 13. (1) За дейностите по обработване на личните данни, посочени в чл. 5 за целите, посочени в чл. 6, **ФОНДАЦИЯ „КЕРА”** води регистри с всички категории дейности по обработване.

(2) ФОНДАЦИЯ „КЕРА” води поотделно следните регистри:

1. Регистър „Членове”

2. Регистър „Трети външни лица”

(3) Всеки от регистрите съдържа следната информация:

1. наименованието и координатите за връзка на администратора, и когато е приложимо, на съвместните администратори и на длъжностното лице по защитата на данните;

2. целите на обработването;

3. категориите получатели, пред които са или ще бъдат разкрити личните данни, включително получателите в трети държави или международни организации;

4. описание на категориите субекти на данни и на категориите лични данни;

5. когато е приложимо, използването на профилиране;

6. когато е приложимо, категориите предаване на лични данни на трета държава или международна организация;

7. посочване на правното основание за операцията по обработване, включително предаването на данни, за която са предназначени личните данни;

8. когато е възможно, предвидените срокове за изтриване на различните

категории лични данни;

9. когато е възможно, общо описание на техническите и организационните мерки за сигурност .

(4) Регистрите, посочени в ал. 1, се поддържат в писмена форма, в електронен формат.

ОЦЕНКА НА ВЪЗДЕЙСТВИЕ

Чл. 14. (1) Когато съществува вероятност определен вид обработване, по-специално при което се използват нови технологии, и предвид естеството, обхвата, контекста и целите на обработването, да породи висок риск за правата и свободите на физическите лица, преди да бъде извършено обработването, **ФОНДАЦИЯ „КЕРА”** извършва оценка на въздействието на предвидените операции по обработването върху защитата на личните данни.

(2) Оценката по ал. 1 съдържа най-малко общо описание на предвидените операции по обработване, оценка на рисковете за правата и свободите на субектите на данните, мерките, предвидени за справяне с тези рискове, гаранции, мерки за сигурност и механизми за гарантиране на защитата на личните данни и за доказване на съответствие с правилата на защита на личните данни съгласно Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица (Общ регламент относно защитата на данните), на Закона за защита на личните данни (ЗЗЛД) и подзаконовите нормативни актове, приети за неговото изпълнение, като се вземат предвид правата и легитимните интереси на субектите на данните и другите засегнати лица.

(3) Когато оценката на въздействието покаже, че обработването ще породи висок риск по смисъла на Общия регламент относно защитата на данните, на Закона за защита на личните данни (ЗЗЛД) и подзаконовите нормативни актове, приети за неговото изпълнение, управителят на **ФОНДАЦИЯ „КЕРА”** се консултира с Комисията за защита на личните данни преди извършване на обработването.

ЗАДЪЛЖЕНИЯ НА АДМИНИСТРАТОРА НА ЛИЧНИ ДАННИ

Чл. 15. (1) Прилагането на предвидените в настоящите правила технически и организационни мерки за защита на личните данни се осъществява от управителя на **ФОНДАЦИЯ „КЕРА”.**

(2) Съпредстедател на Управителния съвет може да определи едно или повече лица по защита на личните данни, които отговарят за координиране и прилагане на мерките по защита на личните данни.

Чл. 16. Съпредстедател на Управителния съвет или определеното от него лице имат следните задължения:

1. приемат, изменият и допълват настоящия Правилник за определяне на технически и организационни мерки и видовете защита на личните данни в организацията и осъществява контрол за спазването и изпълнението му;

2. инструктира лицата, които обработват лични данни по указание на управителя;

3. осигурява организацията по водене на регистрите, прилагане на мерки за защитата им и актуализацията им;

4. извършва оценка на въздействието по чл. 15;

5. уведомява КЗЛД за нарушение на сигурността на личните данни без ненужно забавяне по възможност не по-късно от 72 часа след узнаването и при спазване на изискванията на чл. 33 от Общия регламент относно защитата на данните и Закона за защита на личните данни;

6. съобщава на субекта на данните за нарушението на сигурността на личните му данни, когато има вероятност нарушението на сигурността на личните данни да породи висок риск за правата и свободите на субекта.

7. определя длъжностното лице по защита на данните, в случай, че такова следва да бъде назначено в организацията съгласно изискванията на чл 37 от Общия регламент относно защитата на данните и Закона за защита на личните данни;

8. изисква и следи за спазването на политиката на поверителност от обработващи лични данни;

9. изисква и следи за спазването на правата на субектите на лични данни.

ПРАВА НА СУБЕКТИТЕ НА ДАННИ

Чл. 17. (1) Субектът на данни има следните права по отношение на обработването на данни, както и на данните, които се записват за него:

- Да отправя искания за потвърждаване дали се обработват лични данни, свързани с него, и ако това е така, да получи достъп до данните, както и информация кои са получателите на тези данни.
- Да поиска копие от своите лични данни;
- Да иска коригиране на лични данни когато те са неточни, както и когато не са вече актуални;
- Да изиска изтриване на лични данни (право „да бъдеш забравен");
- Да иска ограничаване на обработването на лични данни доколкото е възможно, като в този случай данните ще бъдат само съхранявани, но не и обработвани;
- Да направи възражение срещу обработване на негови лични данни;
- Да направи възражение срещу обработване на лични данни, отнасящо се до него за целите на директния маркетинг, когато не е дал съгласие за това.
- Да се обърне с жалба до надзорен орган ако смята, че някоя от разпоредбите на Общия регламент относно защитата на данните и Закона за защита на личните данни е нарушена;
- Да поиска и да му бъдат предоставени личните данни в структуриран, широко използван и пригоден за машинно четене формат;
- Да оттегли съгласието си за обработката на личните данни по всяко време с отделно искане, отправено до управителя на **ФОНДАЦИЯ „КЕРА";**

(2) ФОНДАЦИЯ „КЕРА" осигурява условия, които да гарантират упражняването на тези права от субекта на данни:

1. информацията относно обработването се предоставя на субекта на данни сбита, разбираема и леснодостъпна форма, като се използва ясен и прост език. Информацията се предоставя по всякакъв подходящ начин, включително по

електронен път. По възможност информацията се предоставя в същата форма като тази на искането.

2. субекта на данните се информира писмено и без излишно забавяне за действията, предприети във връзка с неговото искане. Информацията се предоставя безплатно. Когато исканията от даден субект на данни са очевидно неоснователни или прекомерни, по-специално поради своята повторяемост, информацията може да бъде предоставена срещу такса в разумен размер, като взема предвид административните разходи за предоставянето ѝ или да се откаже предоставянето ѝ.

3. Когато са налице основателни опасения във връзка със самоличността на физическото лице, което подава искане, може да се изиска допълнителна информация от лицето, необходима за потвърждаване на самоличността му.

(3) ФОНДАЦИЯ „КЕРА” предоставя на субектите на данни най-малко следната информация:

1. данните, които идентифицират администратора и координатите за връзка с него;

2. координатите за връзка с длъжностното лице по защита на данните, когато е приложимо;

3. целите на обработването, за които са предназначени личните данни;

4. правото да бъде подадена жалба до комисията и нейните координати за връзка;

5. съществуването на право да се изиска от администратора достъп до, коригиране или изтриване на лични данни и ограничаване на обработването на лични данни, свързано със субекта на данните.

(4) Освен информацията, посочена в ал. 3, **ФОНДАЦИЯ „КЕРА”** предоставя на субекта на данните, в конкретни случаи и с цел да му се даде възможност да упражни правата си, следната допълнителна информация:

1. правното основание за обработването;

2. срока, за който ще се съхраняват личните данни, а ако това е невъзможно -

критериите, използвани за определяне на този срок;

3. когато е приложимо, категориите получатели на личните данни, включително в трети държави или международни организации;

4. ако е необходимо, и друга допълнителна информация, по-специално в случаите, когато личните данни са събрани без знанието на субекта на данните.

(5) ФОНДАЦИЯ „КЕРА” може да забави, да ограничи или да не предостави информация на субекта на данните, като се отчитат основните права и легитимните интереси на засегнатото физическо лице, за да:

1. не се допусне възпрепятстването на служебни или законово регламентирани проверки, разследвания или процедури;

2. не се допусне неблагоприятно засягане на предотвратяването, разкриването, разследването или наказателното преследване на престъпления или изпълнението на наказания;

3. се защити общественият ред и сигурност;

4. се защити националната сигурност;

5. се защитят правата и свободите на други лица.

След отпадане на съответното обстоятелство по ал. 5 исканата информация се предоставя без забавяне.

ВЪЗЛАГАНЕ ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ НА ОБРАБОТВАЩ

Чл. 18 (1) ФОНДАЦИЯ „КЕРА” може да възложи обработване на лични данни от негово име само на обработващи лични данни, които предоставят достатъчни гаранции, че ще прилагат подходящи технически и организационни мерки, по такъв начин че обработването да отговаря на изискванията на Общия регламент за защита на данните (Регламент (ЕС) 2016/679), на Закона за защита на личните данни, на подзаконовите нормативни актове по прилагането му, както и на настоящия правилник и да се гарантира защитата на правата на субекта на данни.

(2) Обработващият лични данни не може да добавя друг обработващ лични данни без предварителното конкретно или общо писмено разрешение на управителя

на **ФОНДАЦИЯ „КЕРА”.**

(3) Обработването от страна на обработващия лични данни се урежда с договор, който обвързва обработващия лични данни и регламентира предмета и срока на обработването, естеството и целта на обработването, вида лични данни и категориите субекти на данни, задълженията и правата на **ФОНДАЦИЯ „КЕРА”** като администратор. Посоченият договор или друг правен акт предвижда по-специално, че обработващият лични данни:

1. действа единствено по указания на администратора на лични данни;
2. гарантира, че лицата, оправомощени да обработват личните данни, са поели ангажимент за поверителност или са задължени по закон да спазват поверителност;
3. подпомага **ФОНДАЦИЯ „КЕРА”** с всички подходящи средства, за да се гарантира спазването на разпоредбите относно правата на субекта на данни;
4. по избор на **ФОНДАЦИЯ „КЕРА”** заличава или връща всички лични данни след приключване на предоставянето на услуги по обработване на данни и заличава съществуващите копия, освен ако правото на Европейския съюз или законодателството на Република България не изисква съхранение на личните данни;
5. предоставя на **ФОНДАЦИЯ „КЕРА”** цялата информация, необходима за доказване на спазването на настоящия член;
6. спазва условията по алинеи 2 за включване на друг обработващ лични данни.

(4) Договорът се изготвя в писмена или електронна форма.

(5) Ако обработващ лични данни определи в нарушение на правилата на настоящата глава целите и средствата на обработването, обработващият личните данни се счита за администратор по отношение на това обработване.

(6) Обработващият лични данни и всяко лице, действащо под ръководството на **ФОНДАЦИЯ „КЕРА”** или на обработващия лични данни, което има достъп до личните данни, обработва тези данни само по указание на **ФОНДАЦИЯ „КЕРА”**, освен ако обработването се изисква от правото на ЕС или законодателството на Република България.

РАЗКРИВАНЕ НА ДАННИ

Чл.19.(1) ФОНДАЦИЯ „КЕРА” не разкрива и предприема мерки, за да не бъдат разкривани от негови служители лични данни 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, занимаващи се с обработка на лични данни се инструктират да бъдат предпазливи, когато им поискат да разкрият съхранявани лични данни за друго лице на трета страна. В случаи на съмнения и неяснота, следва да се обръщат към управителя на **ФОНДАЦИЯ „КЕРА”.**

(2) 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 Управителя на **ФОНДАЦИЯ „КЕРА”** или от Длъжностното лице за защита на данните / Отговорникът за защита на данните, ако са назначени такива.

СЪХРАНЯВАНЕ И УНИЩОЖАВАНЕ НА ДАННИТЕ

Чл. 20.(1) ФОНДАЦИЯ „КЕРА” 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**.**

(2) Личните данни трябва се унищожават 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 (принцип на цялостност и поверителност).

ТРАНСФЕР НА ДАННИ

Чл. 21.(1) Всеки износ на данни извън ЕС е незаконен, освен ако няма подходящо ниво на защита на основните права на субектите на данни, което се

проверява и удостоверява от управителя.

(2) Прехвърлянето на лични данни извън ЕС е забранено, освен ако не се прилагат една или повече от гаранциите или изключенията, посочени в чл. 44-50 от Общия регламент.

(3) ФОНДАЦИЯ „КЕРА” може да включи утвърдени стандартни договорни клаузи за защита на данните при прехвърляне на данни извън Европейското икономическо пространство, одобрени от КЗЛД с оглед автоматичното признаване на адекватността им.

(4) При липса на гаранциите, посочени в чл. 44-48 от Общия регламент, прехвърляне на лични данни в трета страна или международна организация се извършва само при едно от следните условия:

- субектът на данните изрично се е съгласил с предложеното 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 или за изпълнението на преддоговорни мерки, взети по искане на субекта на данните;
- предаването е необходимо за сключването или изпълнението на договор, сключен в интерес на субекта на данните между администратора и друго физическо или юридическо лице;
- 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;
- предаването се извършва от регистър, който съгласно правото на ЕС или правото на държавите членки е предназначен да предоставя информация на обществеността и е достъпен за справка от обществеността по принцип или от всяко лице, което може да докаже, че има законен интерес за това, но само доколкото условията за справка, установени в правото на Съюза или правото на държавите

членки, са изпълнени в конкретния случай.

ДОПЪЛНИТЕЛНА РАЗПОРЕДБА

§ 1. По смисъла на този правилник:

„ЛИЧНИ ДАННИ" - всяка информация, свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано („субект на данни"); физическо лице, което може да бъде идентифицирано, е лице, което може да бъде идентифицирано, пряко или непряко, 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;

„СПЕЦИАЛНИ КАТЕГОРИИ ЛИЧНИ ДАННИ“ – лични данни, разкриващи расов или етнически произход, политически възгледи, религиозни или философски убеждения, или членство в синдикални организации и обработката на генетични данни, биометричните данни за уникално идентифициране на физическо лице, данни отнасящи се до здравето или данни относно сексуалния живот на физическо лице или сексуална ориентация.
„ДАННИ ЗА ЗДРАВОСЛОВНОТО СЪСТОЯНИЕ“ означава лични данни, свързани с физическото или психическото здраве на физическо лице, включително предоставянето на здравни услуги, които дават информация за здравословното му състояние;

„ДЕТЕ“ – Общият Регламент определя дете като всеки на възраст под 16 години въпреки че това може да бъде намалена на 13 от правото на държавата-членка. Обработката на лични данни на едно дете е законно само, ако родител или попечител е дал съгласие. Администраторът полага разумни усилия, за да провери в такива случаи, че притежателят на родителската отговорност за детето е дал или упълномощен да даде съгласието си;

„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;

„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;

„СУБЕКТ НА ДАННИТЕ“ – всяко живо физическо лице, което е предмет на личните данни съхранявани от Администратора;
„СЪГЛАСИЕ” - всяко свободно изразено, конкретно, информирано и недвусмислено указание за волята на субекта на данните, посредством изявление или ясно потвърждаващо действие, което изразява съгласието му свързаните с него лични данни да бъдат обработени;
„НАРУШЕНИЕ НА СИГУРНОСТТА НА ЛИЧНИ ДАННИ” - 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;

„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 Съюза 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 ръководство на администратора или на обработващия лични данни имат право да обработват личните данни;

„РЕГИСТЪР С ЛИЧНИ ДАННИ“ означава всеки структуриран набор от лични данни, достъпът до които се осъществява съгласно определени критерии, независимо дали е централизиран, децентрализиран или разпределен съгласно функционален или географски принцип;

„НАДЗОРЕН ОРГАН“ означава независим публичен орган от държава членка на Европейския съюз, отговорен за наблюдението на прилагането на правилата за защита на личните данни, с които са въведени разпоредбите на Директива 2016/680 в съответното национално законодателство, с цел да се защитят основните права и свободи на физическите лица във връзка с обработването на лични данни и да се улесни свободното им движение в рамките на ЕС. За Република България надзорен орган е Комисията за защита на личните данни:

КОМИСИЯ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

Адрес: София 1592, бул. „Проф. Цветан Лазаров” № 2
Център за информация и контакти - тел. 02/91-53-518
Приемна - работно време 9:00 - 17:30 ч.
Електронна поща: kzld@cpdp.bg
Интернет страница: www.cpdp.bg