

**Основни положения от
ПРАВИЛА ЗА ПОВЕДЕНИЕ**

на „ЛАРИС“ МЛС ООД за прилагане на Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (GDPR)

🚩 ОБЩИ ПОЛОЖЕНИЯ

Този документ определя правилата за поведение на „ЛАРИС МЛС“ ООД (Администраторът), ЕИК 205026969, с адрес: гр. София, бул. „Андрей Ляпчев“ № 51 – администратор на лични данни по смисъла на ЗЗЛД и ОРЗЛД, относно мерките за защита на личните данни. Задължаваме се да използваме разписаните добри практики при събирането, обработването, съхранението и преносимостта, определени в РЕГЛАМЕНТ (ЕС) 2016/679.

🚩 ЦЕЛ:

Ръководството на дружеството има за цел да допринесе за правилното прилагане на РЕГЛАМЕНТА, като отчитаме специфичните характеристики на служителите ни, обработващи данните, а също така и особеностите на потребителите на услугите, които предоставяме. Основна цел е осигуряването на механизми за защита на личните данни и тяхната неприкосновеност.

🚩 ОБХВАТ

РЕГЛАМЕНТЪТ се прилага за обработването на лични данни частично с автоматични средства, както и за обработването с други средства, които са част от регистрите с лични данни или са предназначени да съставляват част от друг регистър.

Териториален обхват

РЕГЛАМЕНТЪТ се прилага за обработването на лични данни в контекста на дейностите на организацията, на установяването на администратора или обработващия лични данни в организацията, независимо дали обработването се извършва в нея или не.

🚩 ОПРЕДЕЛЕНИЯ

Ние се съобразяваме със следните определения, посочени в регламента:

„лични данни“	всяка информация, свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано.
„субект на данни“	лице, което може да бъде идентифицирано, пряко или непряко, по-специално чрез идентификатор като име, идентификационен номер, данни за местонахождение, онлайн идентификатор
„обработване“	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.
„ограничаване на обработването“	Маркиране на съхранявани лични данни с цел ограничаване на обработването им в бъдеще
„профилиране“	всяка форма на автоматизирано обработване на лични данни, изразяващо се в използването на лични данни за оценяване на определени лични аспекти, свързани с физическо лице
„псевдонимизация“	обработването на лични данни по такъв начин, че те да не могат повече да бъдат свързвани с конкретен субект на данни, без да се използва допълнителна информация, при условие че тя се съхранява отделно.

„регистър с лични данни“	всеки структуриран набор от лични данни, достъпът до които се осъществява съгласно критерии, независимо дали е централизиран, децентрализиран
„администратор“	физическо или юридическо лице, което само или съвместно с други определя целите и средствата за обработването на лични данни
„обработващ лични данни“	физическо или юридическо лице, което обработва лични данни от името на администратора
„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
„съгласие на субекта на данните“	Всяко свободно изразено, конкретно указание за волята на субекта на данните, посредством изявление за изразяване съгласието му свързаните с него лични данни да бъдат обработени
„трета страна“	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
„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
„представител“	физическо или юридическо лице, установено в Съюза, което, назначено от администратора или обработващия лични данни в писмена форма съгласно член 27, представлява администратора или обработващия лични данни във връзка със съответните им задължения по настоящия регламент
„дружество“	Физическо или юридическо лице, което осъществява икономическа дейност, независимо от правната му форма, включително партньорствата или сдруженията, които редовно осъществяват икономическа дейност
„задължителни фирмени правила“	политики за защита на личните данни, които се спазват от администратор или обработващ лични данни, установен на територията на държава членка, при предаване или съвкупност от предавания на лични данни до администратор или обработващ лични данни в една или повече трети държави в рамките на група предприятия или група дружества, участващи в съвместна стопанска дейност
„надзорен орган“	означава независим публичен орган, създаден от държава членка, съгласно член 51 от Регламента
„засегнат надзорен орган“	надзорен орган, който е засегнат от обработването на лични данни, тъй като: а) администраторът или обработващият лични данни е установен на територията на държавата членка на този надзорен орган; б) субектите на данни с местопребиваване в държавата членка на този надзорен орган са засегнати съществено или е вероятно да бъдат засегнати съществено от обработването; или в) до този надзорен орган е подадена жалба;

ПРИНЦИПИ

Нашата организация се задължава да спазва при обработването на лични данни следните принципи, залегнали в Регламента:

Законосъобразност; Добросъвестност; Прозрачност	Личните данни са обработвани законосъобразно, добросъвестно и по прозрачен начин по отношение на субекта на данните
Ограничение на целите	Събират се за конкретни, изрично указани и легитимни цели и не се обработват по-нататък по начин, несъвместим с тези цели; по-нататъшното обработване за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели не се счита, за несъвместимо с първоначалните цели
Точност	Данните са точни и при необходимост са поддържани в актуален вид; трябва да се предприемат всички разумни мерки, за да се гарантира своевременното изтриване или коригиране на неточни лични данни, като се имат предвид целите, за които те се обработват
Ограничение на съхраненото	Съхраняват се 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; Личните данни могат да се съхраняват за по-дълги срокове, доколкото ще бъдат обработвани единствено за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели, при условие че бъдат приложени подходящите технически и организационни мерки, предвидени в настоящия РЕГЛАМЕНТ с цел да бъдат гарантирани правата и свободите на субекта на данните
Цялостност и поверителност	Обработват се по начин, който гарантира подходящо ниво на сигурност на личните данни, включително защита срещу неразрешено или незаконосъобразно обработване и срещу случайна загуба, унищожаване или повреждане, като се прилагат подходящи технически или организационни мерки
Отчетност	Администраторът носи отговорност и трябва да е в състояние да докаже спазването му

Законосъобразност на обработването

Обработването е законосъобразно, само ако е приложимо към поне едно от следните условия:

- субектът на данните е дал съгласие за обработване на личните му данни;
- обработването е необходимо за изпълнението на договор, по който субектът на данните е страна;
- обработването е необходимо за спазването на законово задължение, което се прилага спрямо администратора;
- обработването е необходимо, за да бъдат защитени жизненоважните интереси на субекта на данните или на друго физическо лице;
- обработването е необходимо за изпълнението на задача от обществен интерес или при упражняването на официални правомощия, които са предоставени на администратора;
- обработването е необходимо за целите на легитимните интереси на администратора.

🚩 УСЛОВИЯ

➤ Условие за даване на съгласие

При нас, събирането и обработването на личните данни се извършва на основание легитимни интереси и като необходимо условие за извършване на заявена от Вас регистрация в laris.bg и

заявените от вас услуги. Осигурен е достъп на субектите на данни до политиките за поверителност, отнасящи се до касаещите ги дейности, за нуждите на които се събират и обработват лични данни, където е представена информация, която се отнася до обработването, на данните в кратка, прозрачна, разбираема и лесно достъпна форма, на ясен и прост език. Информацията се предоставя писмено и с електронни средства. Субектите на данни декларират, че са запознати с Правила за поведение на „ЛАРИС“ МЛС ООД за прилагане на Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (GDPR), както и с правата си по отношение на предоставените лични данни.

Субектът на данни има правото да оттегли съгласието си по всяко време. Оттеглянето на съгласието не засяга законосъобразността на обработването, основано на дадено съгласие преди неговото оттегляне. Преди да даде съгласие, субектът на данни ще бъде информиран за това.

➤ **Условия, приложими за съгласието на дете във връзка с услугите, предоставяни от „ЛАРИС МЛС“ ООД**

Предвид спецификата на дейността ни, обработването на лични данни, свързани с дете, се извършва съгласно предвидените от законодателството случаи. В тези случаи са създадени условия за удостоверяване, че съгласието е дадено или разрешено от носещия родителска отговорност за детето.

ОБРАБОТВАНЕ

➤ **Обработване на лични данни, във връзка с дейностите ни**

Предоставяне на лични данни свързани с различни видове услуги за клиенти на „ЛАРИС МЛС“ ООД. При обработка на предоставената от субектите на данни информация, ние се позоваваме на основание „**легитимен интерес**“, като гарантираме справедлив баланс между легитимните интереси и правата на потребителите на услуги като регистрирани потребители в laris.bg. Най-често събираме и обработваме идентификационни данни като:

Три имена;

Адрес;

Информация за контакт (личен имейл адрес, домашен и/или мобилен телефонен номер, работен телефонен номер, работен имейл адрес);

В случай, че регистрираните потребители – субекти на лични данни, предоставят данни или документи, съдържащи лични данни на трети лица, то субектите са задължени да декларират и гарантират, че последните са събрани законосъобразно, и при споделянето им с други регистрирани потребители в информационните системи на „ЛАРИС МЛС“ ООД носят пълната отговорност за своите действия.

Достъп до файловете за обработка на лични данни имат само определените от ръководството лица. Осигурена е защита от вътрешен и външен неправомерен достъп.

ПРАВА НА СУБЕКТА НА ДАННИ

При нас са предприети необходимите мерки за предоставяне на всякаква информация и комуникация, която се отнася до обработването на данните в кратка, прозрачна, разбираема и лесно достъпна форма, на ясен и прост език.

Информацията се предоставя писмено или по друг начин, включително, когато е целесъобразно, с електронни средства. Ако субектът на данните е поискал това, информацията може да бъде дадена устно, при положение, че идентичността на субекта на данните е доказана с други средства.

Фирмата, в качеството си на администратор, съдейства за упражняването на правата на субекта на данните и не отказва да предприеме действия по искане на субекта на данните за упражняване на правата му, освен ако докаже, че не е в състояние да идентифицира субекта на данните.

Администраторът предоставя на субекта на данни информация относно действията, предприети, без ненужно забавяне и в срок от един месец от получаване на искането. При необходимост този срок може да бъде удължен с още два месеца, като се взема предвид сложността и броя на исканията. Администраторът информира субекта на данните за всяко такова удължаване в срок от един месец от получаване на искането, като посочва и причините за забавянето. Когато субектът на данни подава искане с електронни средства, по възможност информацията се предоставя с електронни средства, освен ако субектът на данни не е поискал друго.

Ако Администраторът не предприеме действия по искането на субекта на данни, уведомява субекта на данни, без забавяне и най-късно в срок от един месец от получаване на искането, за причините да не предприеме действия и за възможността за подаване на жалба до надзорен орган и търсене на защита по съдебен ред.

➤ **Информация, предоставяна при събиране на лични данни от субекта на данните**

Когато лични данни, свързани с даден субект на данни, се събират от субекта на данните, в момента на получаване на личните данни Организацията, в качеството си на администратор, предоставя на субекта на данните цялата посочена по-долу информация:

- ✓ данните, които идентифицират администратора и координатите за връзка с него и, когато е приложимо, тези на представителя на администратора;
- ✓ координатите за връзка с Длъжностното лице по защита на личните данни;
- ✓ целите на обработването, за което личните данни са предназначени, както и правното основание за обработването;
- ✓ получателите или категориите получатели на личните данни.

Освен информацията, посочена по-горе, в момента на получаване на личните данни администраторът предоставя на субекта на данните следната допълнителна информация, която е необходима за осигуряване на добросъвестно и прозрачно обработване:

- ✓ срокът, за който ще се съхраняват личните данни, а ако това е невъзможно, критериите, използвани за определяне на този срок;
- ✓ съществуването на право да се изиска от администратора достъп до, коригиране или изтриване на лични данни или ограничаване на обработването на лични данни, свързани със субекта на данните, или право да се направи възражение срещу обработването, както и правото на преносимост на данните;
- ✓ правото на жалба до надзорен орган;
- ✓ дали предоставянето на лични данни е задължително или договорно изискване, или изискване, необходимо за сключването на договор, както и дали субектът на данните е длъжен да предостави личните данни и евентуалните последствия, ако тези данни не бъдат предоставени;

Ние имаме готовност, в случай че се наложи да обработваме предоставените лични данни за цел различна от тази, за която са събрани, да предоставим на субекта на данните преди това по-нататъшно обработване информация за тази друга цел и всякаква друга необходима информация.

Администраторът предоставя информацията, посочена по-горе:

- ✓ в разумен срок след получаването на личните данни, но най-късно в срок до един месец, като се отчитат конкретните обстоятелства, при които личните данни се обработват;
- ✓ ако данните се използват за връзка със субекта на данните, най-късно при осъществяване на първия контакт с този субект на данните;
- ✓ ако е предвидено разкриване пред друг получател, най-късно при разкриването на личните данни за първи път.

Изброените дейности на администратора не се прилагат, когато:

- ✓ субектът на данните вече разполага с информацията;
- ✓ предоставянето на такава информация се окаже невъзможно или изисква несъразмерно големи усилия по-специално за обработване на данни за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели;
- ✓ получаването или разкриването е изрично разрешено от правото на Съюза или правото на Р. България, което се прилага спрямо администратора и в което се предвиждат също подходящи мерки за защита на легитимните интереси на субекта на данните;
- ✓ личните данни трябва да останат поверителни при спазване на задължение за опазване на професионална тайна, което се урежда от правото на Съюза или право на Р. България, включително законово задължение за поверителност.

➤ **Право на достъп на субекта на данните**

Субектът на данните има право да получи от администратора потвърждение дали се обработват лични данни, свързани с него, и ако това е така, да получи достъп до данните и информацията, свързана с тях.

Когато личните данни се предават на трета държава или на международна организация, субектът на данните има право да бъде информиран относно подходящите гаранции във връзка с предаването.

➤ **Коригиране и изтриване**

Субектът на данни има право да поиска от администратора 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, включително чрез добавяне на декларация.

➤ **Право на изтриване (право "да бъдеш забравен")**

Субектът на данни има правото да поиска от администратора изтриване на свързаните с него лични данни без ненужно забавяне, а администраторът има задължението да изтрие без ненужно забавяне личните данни.

➤ **Право на ограничаване на обработването**

Подаващия данните има право да изиска от администратора ограничаване на обработването.

➤ **Задължение за уведомяване при коригиране или изтриване на лични данни или ограничаване на обработването.**

Администраторът съобщава за всяко извършено коригиране, изтриване или ограничаване на обработване на всеки получател, на когото личните данни са били разкрити, освен ако това е невъзможно или изисква несъразмерно големи усилия. Администраторът информира субекта на данните относно тези получатели, ако субектът на данните поиска това.

➤ **Право на преносимост на данните**

Субектът на данните има право да получи личните данни, които го засягат и които той е предоставил на администратора, в структуриран, широко използван и пригоден за машинно четене формат и има правото да прехвърли тези данни на друг администратор без възпрепятстване от администратора. Когато упражнява правото си на преносимост на данните, субектът на данните има право да получи пряко прехвърляне на личните данни от един администратор към друг, когато това е технически осъществимо.

➤ **Право на възражение**

Субектът има право, по всяко време и на основания, свързани с неговата конкретна ситуация, на възражение срещу обработване на лични данни, отнасящи се до него, включително и профилиране, Администраторът прекратява обработването на личните данни, освен ако не докаже, че съществуват убедителни законови основания за обработването, които имат

предимство пред интересите, правата и свободите на субекта на данни, или за установяването, упражняването или защитата на правни претенции.

Най-късно в момента на първото осъществяване на контакт със субекта на данните, той изрично се уведомява за съществуването на правото, което му се представя по ясен начин и отделно от всяка друга информация.

➤ **Автоматизирано вземане на индивидуални решения, включително профилиране**

Организацията, в качеството си на администратор, информира субекта на данни че има право да не бъде обект на решение, основаващо се единствено на автоматизирано обработване.

➤ **Ограничения**

В правото на Съюза или правото на Р. България, което се прилага спрямо администратора или обработващия лични данни, чрез законодателна мярка може да се ограничи обхватът на задълженията и правата, предвидени в неговите разпоредби и съответстват на правата и задълженията, когато подобно ограничение е съобразено със същността на основните права и свободи и представлява необходима и пропорционална мярка в едно демократично общество с цел да се гарантира:

- ✓ националната сигурност;
- ✓ отбраната;
- ✓ обществената сигурност;
- ✓ предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наложените наказания, включително предпазването от и предотвратяването на заплахи за обществената сигурност;
- ✓ други важни цели от широк обществен интерес за Съюза или за Р България, и по-специално важен икономически или финансов интерес на Съюза или на Р България, включително паричните, бюджетните и данъчните въпроси, общественото здраве и социалната сигурност;
- ✓ защитата на независимостта на съдебната власт и съдебните производства;
- ✓ предотвратяването, разследването, разкриването и наказателното преследване на нарушения на етичните кодекси при регламентираните професии;
- ✓ функция по наблюдението, проверката или регламентирането, свързана, дори само понякога, с упражняването на официални правомощия
- ✓ защитата на субекта на данните или на правата и свободите на други лица;
- ✓ изпълнението по гражданско-правни искове.

Задължения и отговорности

➤ **Отговорност на администратора**

Като взема предвид естеството, обхвата, контекста и целите на обработването, както и рисковете с различна вероятност и тежест за правата и свободите на физическите лица, при нас са въведени подходящи технически и организационни мерки, за да гарантира, че обработването се извършва в съответствие с РЕГЛАМЕНТА. Тези мерки се преразглеждат и при необходимост се актуализират.

Посочените по-горе мерки включват прилагане от страна на администратора на подходящи Политики по сигурност.

Придържането към одобрени правила за поведение, може да се използва като елемент за доказване на спазването на задълженията на администратора.

➤ **Защита на данните на етапа на проектирането и по подразбиране**

Като взема предвид контекста и целите на обработването, както и породените от обработването рискове с различна вероятност и тежест за правата и свободите на физическите лица, в „ЛАРИС МЛС“ ООД са приети, към момента на самото обработване, подходящи технически и организационни мерки, които са разработени с оглед на ефективното прилагане на принципите за защита на данните - например свеждане на данните до минимум, и интегриране на

необходимите гаранции в процеса на обработване, за да се спазят изискванията на регламента и да се осигури защитят правата на субектите на данни.

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

➤ **Обработващ личните данни**

При нас се използват лица и/или външни администратори на лични данни, обработващи лични данни, които предоставят достатъчни гаранции за прилагането на подходящи технически и организационни мерки по такъв начин, че обработването да протича в съответствие с изискванията на настоящия регламент и да осигурява защита на правата на субектите на данни. Лицата, обработващи лични данни, са запознати със своите задължения и отговорности – Задължения на администратора и обработващия лични данни – и са подписали съответните декларации.

Обработващият данни не включва друг обработващ данни без предварителното конкретно или общо писмено разрешение на администратора. В случай на общо писмено разрешение, обработващият данни винаги информира администратора за всякакви планирани промени за включване или замяна на други лица, обработващи данни, като по този начин даде възможност на администратора да оспори тези промени.

Обработването от страна на обработващия лични данни се урежда с договор или с друг вътрешен акт, който е задължителен за обработващия лични данни спрямо администратора, и който регламентира предмета и срока на действие на обработването, естеството и целта на обработването, вида лични данни и категориите субекти на данни и задълженията и правата на администратора.

➤ **Обработване под ръководството на администратора или обработващия лични данни**

Обработващият лични данни и всяко лице, действащо под ръководството на администратора или на обработващия лични данни, което има достъп до личните данни, обработва тези данни само по указание на администратора, освен ако обработването не се изисква от правото на Съюза или правото на Р. България.

✚ **Сътрудничество с надзорния орган**

При поискване администраторът и обработващият лични данни и техните представители си сътрудничат с надзорния орган при изпълнението на неговите задължения.

✚ **Сигурност на личните данни**

➤ **Сигурност на обработването**

Като има предвид техническите си възможности, разходите за прилагане и естеството, обхватът, контекстът и целите на обработването, както и рисковете с различна вероятност и тежест за правата и свободите на физическите лица, „ЛАРИС МЛС“ ООД, като администратор, и обработващите лични данни или външни администратори на лични данни прилагат подходящи технически и организационни мерки за осигуряване на съобразено с този риск ниво на сигурност, детайлно разписани в Политиките по сигурност, включително, и когато това е целесъобразно:

- ✓ псевдонимизацията и криптирането на личните данни;
- ✓ способността за гарантиране на постоянна поверителност, цялостност, наличност и устойчивост на системите и услугите за обработване;

- ✓ способността за своевременно възстановяване на наличността и достъпа до личните данни в случай на физически или технически инцидент;
- ✓ процесът на редовно тестване, оценка на ефективността на техническите и организационните мерки с оглед да се гарантира сигурността на обработването.

➤ **Уведомяване на надзорния орган за нарушение на сигурността на личните данни**

В случай на нарушение на сигурността на личните данни администраторът, 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, освен ако не съществува вероятност нарушението на сигурността на личните данни да породи риск за правата и свободите на физическите лица. Уведомлението до надзорния орган съдържа причините за забавянето, когато не е подадено в срок от 72 часа.

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

Когато и доколкото не е възможно информацията да се подаде едновременно, информацията може да се подаде поетапно без по-нататъшно ненужно забавяне.

Администраторът документира всяко нарушение на сигурността на личните данни, включително фактите, свързани с нарушението на сигурността на личните данни, последиците от него и предприетите действия за справяне с него. Тази документация дава възможност на надзорния орган да провери дали са спазени изискванията.

➤ **Съобщаване на субекта на данните за нарушение на сигурността на личните данни**

Когато има вероятност нарушението на сигурността на личните данни да породи висок риск за правата и свободите на физическите лица, администраторът, без ненужно забавяне, съобщава на субекта на данните за нарушението на сигурността на личните данни.

В съобщението до субекта на данните, на ясен и прост език се описва естеството на нарушението на сигурността на личните данни и се посочват най-малко информацията и предприетите мерки.

Посоченото съобщение до субекта на данните не се изисква, ако някое от следните условия е изпълнено:

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

Ако администраторът все още не е съобщил на субекта на данните за нарушението на сигурността на личните му данни, надзорният орган може, след като отчете каква е вероятността нарушението на сигурността на личните данни да породи висок риск, да изиска от администратора да съобщи за нарушението или да реши, че е изпълнено някое от условията.

✚ **Оценка на въздействието върху защитата на данните**

Когато съществува вероятност определен вид обработване, при което се използват нови технологии, обхвата, контекста и целите на обработването, може да породи висок риск за правата и свободите на физическите лица. Преди да се направи обработването,

администраторът извършва оценка на въздействието на предвидените операции по обработването върху защитата на личните данни.

Очаква се Надзорният орган да състави и оповести списък на видовете операции по обработване, за които се изисква оценка на въздействието върху защитата на данните.

При необходимост администраторът прави преглед, за да прецени дали обработването е в съответствие с оценката на въздействието върху защитата на данни, най-малкото когато има промяна в риска, с който са свързани операциите по обработване.

➤ **Предварителна консултация**

Администраторът се консултира с надзорния орган преди обработването, когато оценката на въздействието върху защитата на данните покаже, че обработването ще породи висок риск, и ако администраторът не е в състояние да предприеме мерки за ограничаване на риска.

Когато надзорният орган е на мнение, че планираното обработване, нарушава РЕГЛАМЕНТА, особено когато администраторът не е идентифицирал или ограничил риска в достатъчна степен, надзорният орган в срок до осем седмици след получаване на искането за консултация дава писмено становище на администратора или на обработващия лични данни, като може да използва всяко от правомощията си.

✚ **Длъжностно лице по защита на данните**

Администраторът, предвид функциите си на фирмен орган, има ангажимента да определи Длъжностно лице по защита на личните данни.

Длъжностното лице по защита на данните се определя въз основа на неговите професионални качества, и по-специално въз основа на експертните му познания в областта на законодателството и практиките в областта на защитата на данните и способността му да изпълнява задачите.

Длъжностното лице по защита на данните може да бъде член на персонала на администратора или на обработващия лични данни или да изпълнява задачите въз основа на договор за услуги. Отговорностите и пълномощията са разписани в длъжностна характеристика.

Администраторът публикува данните за контакт с длъжностното лице по защита на данните и ги съобщава на надзорния орган.

Администраторът гарантира, че длъжностното лице по защита на данните участва по подходящ начин и своевременно във всички въпроси, свързани със защитата на личните данни. Администраторът и обработващите лични данни подпомагат Длъжностното лице по защита на данните при изпълнението на задачи, като осигуряват ресурсите, необходими за изпълнението на тези задачи, и достъп до личните данни и операциите по обработване, а така също поддържат неговите експертни знания.

Субектите на данни могат да се обръщат към Длъжностното лице по защита на данните по всички въпроси, свързани с обработването на техните лични данни и с упражняването на техните права съгласно настоящия регламент.

Длъжностното лице по защита на данните е длъжно да спазва секретността или поверителността на изпълняваните от него задачи в съответствие с приетите правила.

При изпълнението на своите задачи Длъжностното лице по защита на данните надлежно отчита рисковете, свързани с операциите по обработване, и се съобразява с естеството, обхвата, контекста и целите на обработката.

Контакти на лице, изпълняващо функцията на длъжностно лице по защита на данните: e-mail: office@laris.bg, тел: +359 878 186 768

✚ **Предаване на лични данни на трети държави или международни организации**

Извършваните дейности от **Администратора** и обработването на лични данни във връзка с тези дейности нямат пряко отношение към предаването им на трета държава или на международна организация, както и предавания на лични данни от третата държава или от

международната организация на друга трета държава или на друга международна организация. При възникване на подобна ситуация ще бъдат спазени изискванията на Регламента

✚ Предаване или разкриване на данни, което не е разрешено от правото на Съюза

Всяко решение на съд или трибунал и всяко решение на административен орган на трета държава, с което от администратор се изисква да предаде или разкрие лични данни, могат да бъдат признати или да подлежат на изпълнение по какъвто и да било начин само ако се основават на международно споразумение, като договор за правна взаимопомощ, което е в сила между третата държава, отправила искането, и Съюза или негова държава членка, без да се засягат другите основания за предаване на данни съгласно настоящата глава.

✚ Дерогации в особени случаи

При липса на решение относно адекватното ниво на защита или на подходящи гаранции, включително задължителни фирмени правила, предаване или съвкупност от предавания на лични данни на трета държава или международна организация се извършва при условията определени в Регламента.

✚ Право на подаване на жалба до надзорен орган

Без да се засягат, които и да било други административни или съдебни средства за правна защита, всеки субект на данни има право да подаде жалба до надзорен орган, по-специално в Р. България на обичайно местопребиваване, място на работа или място на предполагаемото нарушение, ако субектът на данни счита, че обработването на лични данни, отнасящи се до него, нарушава разпоредбите на приложимия Регламент.

✚ Право на ефективна съдебна защита срещу надзорен орган

Без да се засягат които и да било други административни или несъдебни средства за защита, всяко физическо и юридическо лице има право на ефективна съдебна защита срещу отнасящо се до него решение със задължителен характер на надзорен орган.

✚ Право на ефективна съдебна защита срещу администратор или обработващ лични данни

Без да се засягат които и да било налични административни или несъдебни средства за защита, включително правото на подаване на жалба до надзорен орган, всеки субект на данни има право на ефективна съдебна защита, когато счита, че правата му, съгласно Регламента са били нарушени в резултат на обработване на личните му данни.

✚ Право на обезщетение и отговорност за причинени вреди

Всяко лице, което е претърпяло материални или нематериални вреди в резултат на нарушение на приложимия Регламент, има право да получи обезщетение. Администраторът, участващ в обработването на лични данни, носи отговорност за вреди, произтичащи от извършеното обработване, което нарушава изискване на Регламента.

Обработващият лични данни носи отговорност за вреди, произтичащи от извършеното обработване, само когато не е изпълнил задълженията по Регламента, конкретно насочени към обработващите лични данни, или когато е действал извън законосъобразните указания на администратора или в противоречие с тях.

➤ Съхраняване, унищожаване и инвентаризация на лични данни

✚ Съхраняване

„ЛАРИС МЛС“ ООД не съхранява лични данни във вид, който позволява идентифицирането на субектите за период, по-дълъг от необходимия за осъществяване на обработването, за което е дадено съгласието на субекта на лични данни (Декларация за информирано съгласие за предоставяне, обработване и съхранение на лични данни) и с оглед на целите, за които са били събрани. Съхраняване на лични данни за по-дълъг период е допустимо и без изричното съгласие

на субекта на данни, ако е предвидено в нормативен акт на вътрешното законодателство или на правото на Европейския съюз.

Администраторът може да съхранява данни за по-дълъг период от необходимия за извършване на обработването, за което е дадено съгласие и в случаите, когато личните данни ще бъдат обработвани за целите на архивиране в обществен интерес, научни или исторически изследвания и за статистически цели, и само при изпълнението на подходящи технически и организационни мерки за гарантиране на правата и свободите на субекта на данните

Периодът за съхраняване на всяка категория лични данни, обособена в отделен регистър, се определя в приета от Администратора процедура. В тази процедура са посочени критериите, използвани за определяне на периода на съхранение, включително всякакви законови задължения вменени на Администратора по отношение съхранение на данните. Обичайният период за съхранение е не по-дълъг от съществуването на профила на потребителя, субект на данни, в laris.bg. След изтичането на този срок, „ЛАРИС МЛС“ ООД полага необходимите грижи да изтрие и унищожи всички данни, без ненужно забавяне (до 30 дни).

Процедурата за съхранение и унищожаване на данните, както и правилата за унищожаване на информацията върху физически носители се прилагат във всички случаи.

Унищожаване

Личните данни трябва да бъдат унищожени сигурно, съгласно принципа за гарантиране на подходящо ниво на сигурност и приетата от Администратора процедура.

Спазването на процедурата е задължително с оглед гарантиране защитата срещу неразрешено или незаконосъобразно обработване и срещу случайна загуба, унищожаване или повреждане на данните, като се прилагат подходящи технически или организационни мерки.

Инвентаризация и оценка на риска

Администраторът извършва инвентаризация на данните и оценка на риска като част от своя подход за справяне с възможните рискове при обработване на събираните лични данни.

При инвентаризацията на данните и при тяхното обработване се извършва оценка на риска на личните данни, чиято методология и елементи са уредени с приета от Дружеството процедура. Определянето на рисковете съгласно тази методология се прилага и по отношение на обработването, предприето от други лица / организации от името на Администратора.

Когато се установи, че вид обработване може да доведе до висок риск за правата и свободите на физическите лица, по-специално с използване на нови технологии, и като се вземат предвид естеството, обхвата, контекста и целите на обработването, преди да пристъпи към обработване, Администраторът извършва Оценка за въздействието върху защитата на личните данни съгласно приетата от Дружеството процедура за оценка на въздействието във връзка със защитата на данните и по заложената в същата процедура Методология за извършване на оценка на въздействието върху защитата на личните данни.

Когато в Оценка на въздействието върху защитата на личните данни е установено/указано, че операциите по обработването водят до висок риск, който Администраторът не може да ограничи с подходящи мерки от гледна точка на налични технологии и разходи за прилагане, преди обработването се осъществява консултация с надзорния орган (КЗЛД).

Администраторът прави периодичен преглед на първоначално инвентаризираните данни, преразглежда вписаната информация в „Регистъра на дейностите по обработване“ с оглед всякакви промени в дейностите на Администратора.

ПРЕДАВАНЕ НА ЛИЧНИ ДАННИ НА ТРЕТИ ЛИЦА

Администраторът на лични данни има право да разкрие обработваните лични данни само на следните изчерпателно изброени категории лица:

- физически лица, за които се отнасят данните
- лица, за които правото на достъп е предвидено в нормативен акт или
- лица, за които правото произтича по силата на договор или съгласие за използване на системите Laris MLS и Laris ERP.

С цел предоставяне на услуги, Администраторът разкрива информация /необходими лични данни/ за изпълнението на поето договорно задължение към субекта на лични данни. Следните лични данни на субекта са видими за останалите регистрирани ползватели на информационните системи Laris MLS и Laris ERP:

- Име;
- Телефон за връзка;
- Адрес на извършване на дейността;
- Електронна поща
- Брой години професионален опит

Администраторът предоставя лични данни на трети страни, които предоставят услуги от негово име въз основа на изрична писмена инструкция/ писмен договор. Тези трети страни нямат право да използват или разкриват данните извън целите, за които са им предоставени, освен когато това е необходимо за извършване на услуги от името на Администратора или за съобразяване със законови изисквания. Целите за обработване на предоставените лични данни са изрично определени в писмената инструкция/ писмения договор, въз основа на който данните са предоставени на третото лице. Третите лица (обработващи на лични данни) са задължени да осигурят необходимите технически и организационни мерки за защита на личните данни, предоставяни от Администратора или по-големи;

При предоставено изрично съгласие от субекта на лични данни, последните могат да бъдат споделени с трети страни въз основа на писмен договор, за техни собствени цели, като например предлагане на продукти и услуги, които могат да представляват интерес за субекта на данни;

Администраторът разкрива лични данни на компетентни органи/ лица с оглед организиране защитата на законните си права и интереси при инициране на заповедни, арбитражни, охранителни, искиви и други производства;

Администраторът разкрива лични данни за субекти, чиито лични данни обработва, когато е задължен за това по закон, подзаконов нормативен акт, международен договор или акт на правото на Европейския съюз, или във връзка със съдебна процедура, в отговор на искане от държавни органи, (например правоприлагащи или разследващи органи), или при съмнение за сериозно и незаконосъобразно засягане законните права и интереси на субектите на правото.

➤ ОБУЧЕНИЕ

Като има предвид уредбата на защитата на личните данни на физически лица и засилените мерки за защита на личните данни, въведени с ОРЗД/ ЗЗЛД, „ЛАРИС МЛС“ ООД отчита необходимостта от провеждане на първоначално и последващо обучение на своя персонал, в задълженията на който е включено обработването на лични данни на физически лица от името на Администратора.

Първоначалното и последващите обучения имат за цел да информират служителите относно установените правила и процедури за спазването на настоящата Политика и приложимата нормативна уредба в сферата на защита на личните данни, както и други въпроси, свързани със защитата на личните данни и неприкосновеността на личния живот.

Чрез обученията на работниците и служителите се цели постигане на тяхната осведоменост относно вече наличните или нововъзникнали изисквания относно защитата на личните данни, както и предприетите от Администратора мерки в съответствие с тях.

Правилата за поведение и Политиките по сигурност в своята цялост представляват вътрешните правила на „ЛАРИС МЛС“, по отношение на личните данни и са задължителни за целия персонал на дружеството.