ПОЛИТИКА ЗА НЕПРИКОСНОВЕНОСТ И ЗАЩИТА НА ДАННИТЕ във връзка с Регламент /ЕС/ 2016/679 на Европейския парламент и на Съвета от 27.04.2016г. относно защита 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 защита на данните/

„ДИЛЕКС“ ООД търговско дружество, вписано в Търговския регистър при Агенция по вписванията с ЕИК 121091723 със седалище и адрес на управление: гр. София, р-н Илинден, ж.к. Света Троица, бл. 373, вх. Б, ет. 2, ап. 29, ИН по ЗДДС 121091723, представлявано от Управителя Милен Станчев Димитров, тел.: +35929887900, e-mail: office@dilex.bg, е Администратор на личните данни, по смисъла на чл. 4 ал. 7 от Регламент /ЕС/ 2016/679 използва обем различни данни, чрез които могат да бъдат идентифицирани лица.

Дружеството е с дейност, инженерни дейности и технически консултации. Предлага и изграждане и поддръжка на електрически инсталации, поддържане и обслужване на пожарогасителни и пожароизвестителни системи, системи за управление на дим, топлина и пожарни кранове.

Надзорен орган

Комисията за защита на личните данни

гр. София - 1592, бул. "Цветан Лазаров" № 2

Работно време – от 09:00 ч. до 17:30 ч., уеб сайт: www.cpdp.bg, e-mail: kzld@cpdp.bg.

1. Общ регламент за защита на данните (Регламент /ЕС/2016/679)

Общият регламент за защита на данните (ОРЗД) регламентира дейността по обработване на лични данни.

2. Легални дефиниции

"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;*

"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, 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 на лични данни**" - *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 Съюза 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.*

"**Обработващ лични данни**" - *физическо или юридическо лице, публичен орган, агенция или друга структура, която обработва лични данни от името на администратора.*

3. „ДИЛЕКС“ ООД

в качеството си на Администратор на лични данни **обработва личните данни:**

- **Самостоятелно,** чрез своите служители, под указания извършват дейности по обработване на лични данни по смисъла на чл. 29 от Регламент /ЕС/ 2016/679;
- **Чрез възлагане на обработващ лични данните,** като „ДИЛЕКС“ ООД определя целите и средствата за обработването на личните данни, при наличие на приложимо правно основание, съгласно изискванията на Закона за защита на личните данни и Регламент /ЕС/ 2016/679.

4. Основни принципи при обработването на лични данни

- **Принцип на законосъобразност, добросъвестност и прозрачност**
- **Принцип „ограничение на целите“**
- **Принцип „свеждане на данните до минимум“**
- **Принцип "точност"**
- **Принцип "ограничение на съхранението"**
- **Принцип "цялостност и поверителност**

„ДИЛЕКС“ ООД носи отговорност и е в състояние да докаже спазването на принципите *("**отчетност**").*

„ДИЛЕКС“ ООД гарантира, че зачита и спазва принципите, при използването на настоящите методи по събиране и обработването на лични данни.

5. Цели на обработване на личните данни

„ДИЛЕКС“ ООД обработва личните данни във връзка с изпълнението на следните цели:

5.1. Управление на човешките ресурси (кандидати за работа, служители и изпълнители по трудови и граждански договори), с оглед:

5.1.1. Индивидуализиране на трудови, служебни и граждански правоотношения;

5.1.2. Изпълнение на нормативните изисквания на Кодекса на труда, Кодекса за социално осигуряване, Закона за счетоводството, Закона за данъците върху доходите на физическите лица, Закона за Националния архивен фонд и др.;

5.1.3. Използване на събраните данни за съответните лица за служебни цели:

а/ за всички дейности, свързани със съществуване, изменение и прекратяване на трудовите и граждански правоотношения;

б/ за изготвяне на всякакви документи на лицата в тази връзка (договори, допълнителни споразумения, документи, удостоверяващи трудов стаж, служебни бележки, справки, удостоверения и др. подобни);

в/ за установяване на връзка с лицето по телефон, за изпращане на кореспонденция, отнасяща се до изпълнение на задълженията му по трудови договори;

г/ за водене на счетоводна отчетност, удържане на дължими данъци и други дейности относно възнагражденията на посочените по-горе лица по трудови, служебни и граждански правоотношения;

5.2. За изпълнение на дейности, свързани със сключване, съществуване, изменение и прекратяване на договорни правоотношения, вкл. за:

- изготвяне на всякакви документи;
- изпълнение на нормативните изисквания на Търговския закон, Закон за счетоводството, Закон за данък добавена стойност, Закон за корпоративното подоходно облагане и др.;
- за установяване на връзка с лицето за контакт по телефон, e-mail или по всякакъв друг законосъобразен начин;
- за доставка и/или приемане на стоки/услуги, за комуникация във връзка с предоставяне и/или получаване на стоки/услуги и за предоставяне на свързаното с тях клиентско обслужване;

• за водене на счетоводна отчетност във връзка с изпълненията по договори, по които Администраторът е страна;

• за обработка на плащания във връзка със сключените договори от Администратора.

6. Категории субекти на данни

Администраторът обработва лични данни на следните субекти:

6.1.персонал (по трудови, граждански договори и кандидати за работа);

6.2.контрагенти (клиенти, доставчици, търговски партньори, подизпълнители, и др.), ако са:

- ***физически лица*** или
- ***техните представители и/или лица за контакт***, ако са юридически лица.

7. Категории лични данни, които се обработват

„ДИЛЕКС“ ООД в качеството си на Администратор обработва следните категории лични данни:

7.1.Данни за персонал (по трудови правоотношения):

• ***идентификационни данни*** – имена, адрес, телефонен номер;

• ***единен граждански номер*** – ЕГН;

• ***образование*** – документ за придобито образование; сертификат за квалификация, когато такива се изискват за длъжността. Данните са необходими с оглед спазване нормативни изисквания за заемане на длъжности от лицата;

• ***трудова дейност*** – Документи за стаж по специалността, професионална квалификация;

• ***семейна идентичност*** – семейно положение. Данните са необходими за реализиране на законоустановените права на лицата за ползване на отпуск за майчинство или бащинство, при запор. Декларация за ползване на данъчни облекчения за деца, ползване на отпуск по чл.157 КТ за изпълнение на граждански, обществени и други задължения (встъпване в брак, кръводаряване, смърт на близък роднина и и др.);

• ***икономическа и финансова информация*** – придобит доход при друг работодател, банкова сметка. Данните са необходими за годишно преизчисляване на данъка по ЗДДФЛ, за изплащане на парично обезщетение за временна неработоспособност и трудово възнаграждение;

• ***данни за здравословното състояние*** – документ за трудоустрояване (*предоставяне на определена закрила на служителите*), болничен лист (*изпращане на болничния в НОИ*);

• ***свидетелство за съдимост*** – когато със закон или нормативен акт се изисква удостоверяването на съдебно минало.

7.2.Данни за персонал (по граждански договори):

• ***идентификационни данни*** – имена, постоянен адрес, телефонен номер;

• ***единен граждански номер*** – ЕГН;

• ***икономическа и финансова информация*** – банкова сметка. Данните са необходими за изплащане на възнаграждение;

Обработването се извършва във връзка със сключването, съществуването, изменението и прекратяването на гражданските договори при прилагане и изпълнение на нормативните изисквания на Търговския закон, Кодекса за социално осигуряване, Данъчно-осигурителния процесуален кодекс, Закона за счетоводството, Закона за задълженията и договорите и др.

7.3.Данни за персонал (кандидати за работа):

„ДИЛЕКС“ ООД обработва лични данни на физически лица при кандидатстване за заемане на свободно работно място в Дружеството, като например:

• ***биографични данни*** – имена, дата на раждане, предишна трудова дейност, образование, квалификация;

• ***информация за контакт*** – адрес, телефонен номер, e-mail адрес;

Администраторът събира и обработва личните данни на основание предприемане на стъпки преди сключване на договор, за изпълнението на който е необходимо спазване на законово задължение във връзка с чл.6 т.1 б „б“ и „в“ от Общия регламент за защита на данните. Лични данни се предоставят от физическото лицето в отговор на обявата за работа (на e-mail: office@dilex.bg, или на хартиен носител, лично или по пощата) и във връзка с изискванията на Кодекса на труда

7.4.Данни за Контрагенти ***(клиенти, доставчици, търговски партньори, подизпълнители, наематели и др.):***

• ***идентификационни данни*** – имена, адрес, телефонен номер, e-mail;

• ***единен граждански номер*** – ЕГН;

• ***икономическа и финансова информация*** – банкова сметка. Данните са необходими за обработка на плащанията;

Администраторът обработва данните в изпълнение на нормативно задължение във връзка със сключването на договор и/или изпълнения на задълженията по сключен договор съгласно разпоредбите на Търговския закон, Закона за счетоводството, Закона за задълженията и договорите, Закона за данъка добавена стойност и др. и условията посочени в търговския договор.

Посочените в т.7.1, 7.2, 7.3 и 7.4 лични данни се обработват в изпълнение на нормативно установено задължение, договор и съгласие / Кодекс на труда, КСО, ЗДДФЛ и други законови и подзаконови актове/ чрез възлагане на обработващ данните – „……“ ООД**,** като „ДИЛЕКС“ ООД определя целите и средствата за обработването на личните данни, при наличие на приложимо правно основание, съгласно изискванията на Регламент /ЕС/ 2016/679.

8. Упражняване на права по чл.15 – 22 на Общия регламент за защита на данни. Ред за упражняване правата на субектите на данни.

Вие имате следните права, в качеството Ви на субект на лични данни, които са определени в чл.15 – 22 от Общи регламент за защита на данни:

♦ право да бъдете информирани

♦ право на достъп ;

♦ право на коригиране на съществуващите данни

♦ право на изтриване на данните ("правото да бъдеш забравен")

♦ право за ограничаване на обработването на данните

♦ право на преносимост на данните

♦ право на възражение ;

♦ права във връзка с автоматизираното обработване на данни и профилирането

Правата могат да бъдат упражнени, чрез искане до „ДИЛЕКС“ ООД, подавано лично или чрез пълномощник, по поща на адрес на администратор или на e-mail: office@dilex.bg на администратор с електронен подпис.

3.Информация относно предприети действия по Искането се предоставя при условия на чл.12 т.3 от Регламент /ЕС/ 2016/679.

4.При опасения във връзка със самоличност на физическото лице, което подава Искането, Администраторът може да поиска предоставяне на допълнителна информация, необходима за потвърждаване на самоличността на субекта на данни.

9. Законосъобразност на обработването. Последици от отказ за предоставяне на лични данни

„ДИЛЕКС“ ООД съхранява и обработва лични данни само на посочените правни основания в зависимост от случая, като документира връзката между основанието и обстоятелствата в съответствие с ОРЗД, а именно:

9.1. Изпълнение на договор

Когато събраните и обработвани данни са необходими **за изпълнението на договор със субекта на данните.** Това основание е приложимо в случаите, когато предоставените данни са важни за изпълнението на договора .

9.2. Законово задължение

Когато личните данни са събирани и обработвани, **за да бъде изпълнено законово задължение.**

9.3. Жизненоважни интереси на субекта на данни или на друго физическо лице

Законосъобразно е да получим и обработим лични данни, ако те са необходими за защита на жизненоважни интереси на субекта на данни или на друго физическо лице. „ДИЛЕКС“ ООД ще обработва лични данни на това основание само в случай, че наистина са засегнати жизненоважни интереси, като обстоятелствата ще бъдат детайлно документирани, така че да бъде доказуемо.

9.4. Изпълнение на задача от обществен интерес

Когато „ДИЛЕКС“ ООД трябва да изпълни задача, която вярва, че е в обществен интерес, или е част от служебно задължение, съгласие от субекта на данни няма да бъде поискано. Преценката дали се касае за обществен интерес и/или служебно задължение, се документира и може да служи като доказателство при нужда.

9.5. Легитимен интерес

„ДИЛЕКС“ ООД обработва данни за защита на легитимен интерес, в случай, че не се засягат в значителна степен правата и свободите на субектите на данни. В този случай преценката дали един интерес е легитимен и относно степента на засягане на правата и свободите на субектите на данни ще бъде документирана.

В случай на отказ от предоставяне на изисканите лични данни, „ДИЛЕКС“ ООД няма да бъде в състояние да изпълни свои нормативно установени задължения, включително може да не бъде в състояние да предостави свои услуги/стоки.

10. Защита на етапа на проектиране

„ДИЛЕКС“ ООД зачита принципа за защита на етапа на проектиране. Планирането и изграждането на всички нови или на съществено променени съществуващи системи, които събират, съхраняват или обработват данни, ще бъде оценявано от гледна точка на евентуални проблеми за сигурността. За всеки проект ще бъде правена оценка на въздействието върху защитата на данни и ще бъдат взети подходящите мерки за защита срещу нарушения.

Оценката на въздействието върху защитата на данни включва:

- Преглед на методите за обработка на личните данни и целите;
- Преценка дали очаквания метод за обработка на данни е приложим и подходящ за посочената цел;
- Оценка на риска за субектите на данни при обработване на данните им;

● Какъв контрол и какви мерки за сигурност са необходими, за да се минимизира идентифицирания риск и да се постигне съответствие с изискванията на ОРЗД.
При възможност, ще бъдат използвани техники като псевдонимизиране и съхраняване само на необходимата информация.

11. Предоставяне на личните данни извън дружеството

Личните данни, който се обработват от „ДИЛЕКС“ ООД се предоставят на:

1. физически лица, за които се отнасят данните;
2. на лица, ако е предвидено в нормативен акт – публични органи (Национална агенция за приходите, Национален осигурителен институт, Министерство на вътрешните работи, съдебни органи, контролни органи, органи на местното самоуправление т.н.) в обем, който не надвишава целите, за които са поискани;
3. обработващи лични данни (физическо или юридическо лице, което обработва личните данни от името на администратора и по негово нареждане или възлагане):
   - Служба по трудова медицина
   - Счетоводна къща
4. бизнес партньори – за целите на изпълнение на законово задължение и/или договор;
5. на кредитни институции (банки) - във връзка с изплащането на дължимите възнаграждения на служители и изпълнители по граждански договори;
6. на куриерски фирми и пощенски оператори – за нуждите на осъществяване на кореспонденция с физическите лица-субекти на данни, приемане, пренасяне и доставка и адресиране на пратките до физически лица.

12. Международен трансфер на данни

„ДИЛЕКС“ ООД не предава съхраняваните и обработвани лични данни в трети държави или международни организации.

13. Договори, включващи обработка на лични данни

„ДИЛЕКС“ ООД гарантира, че всички договори, които сключва и в чиито обхват попада обработка на лични данни, ще съдържат необходимата информация и условия, изискуеми от ОРЗД.

14. Срок за съхранение на данните.

Като администратор на данни „ДИЛЕКС“ ООД съхранява и обработва данни за период с минимална продължителност съгласно целите за обработка и предвиденото в действащото законодателство в съответствие с принципа за **ограничаване на съхранението**.

Години	Определяне на срок

50 години	Ведомости за заплати, досиета на персонала – чл.38 от ДОПК
10 години	Счетоводни регистри и финансови отчети, включително документи за данъчен контрол, одит и последващи финансови инспекции – чл.12 от Закон за счетоводството, чл.38 от ДОПК
5 години след изтичане на давностния срок за погасяване на публичното задължение, с което са свързани	Документи за данъчно-осигурителен контрол – чл. 38 от ДОПК
1 месец	Кандидати за работа

15. Длъжностно лице по защита на данните

ОРЗД задължава всяка организация, която е публична, която обработва голям обем лични данни или събира/съхранява "чувствителни" данни да има длъжностно лице по защита на данните. Последното следва да има необходимия обем знания и умения за целите на ОРЗД, но може да бъде както лице от самата организация, така и външно лице.

Съобразно поставените от регламента изисквания, „ДИЛЕКС“ ООД **не трябва** да ангажира длъжностно лице по защита на данните.

16.Технически и организационни мерки за защита на личните данни

Защитата на данните на хартиен и електронен носител от неправомерен достъп, повреждане, изгубване или унищожаване се осигурява посредством вътрешно регулирани технически и организационни мерки:

1. **програмно-технически** – надеждна и защитена идентификация и автентификация на лицата, които обработват лични данни в електронен вид, чрез пароли за достъп и определени потребителски права за работа с данните; поддържане на електронен архив и редовно архивиране на информационните бази, съдържащи лични данни; поддържане на операционните системи и антивирусните програми в актуално състояние.
2. **физически** – система от мерки по защита на помещенията, в които се обработват и съхраняват лични данни и контрола върху достъпа до тях.
3. **организационни и административни** – регламентирани от Управителя на „ДИЛЕКС“ ООД.

17. Уведомление за нарушение на сигурността на данните

В случай на пробив в сигурността на данните, „ДИЛЕКС“ ООД предприема необходимите действия, за да предупреди засегнатите лица.

Действията следва да бъдат пропорционални на нарушението, като следва да се спазва и принципът за прозрачност. ОРЗД задължава организацията, в случай на пробив, който може да застраши правата и свободите на лицата, да уведоми надзорния орган (Комисията за защита на личните данни) в рамките на 72 часа от узнаването.

„ДИЛЕКС“ ООД документира всяко нарушение на сигурността на личните данни, включително фактите, свързани с нарушението, последиците от него и предприетите действия за справяне с него.

18. Постигане на съответствие с ОРЗД

Следните действия са предприети от „ДИЛЕКС“ ООД, за да бъде постигнато пълно съответствие с изискванията на ОРЗД:

- Анализирано е законодателството в областта на личните данни;
- Служителите, които се занимават със събиране и обработване на лични данни, разбират задълженията си и отговорността за спазването на политиките и процедурите за защита на личните данни на организацията;
- Персоналът е инструктиран относно необходимото ниво на защита на данните;
- Предоставени са възможности за упражняване на правата от субектите на данни и техните искания се управляват ефективно;
- Извършват се периодични прегледи с цел актуализация на политиките/процедурите относно защитата на личните данни;
- Спазва се принципът за защита на етапа на проектирането за всички нови или драстично променени системи и процеси;
- Води се следната документация за дейностите по обработване:
  - Името на организацията и други необходими детайли
  - Цели на обработването на данни
  - Категории лица и обработвани техни лични данни
  - Категории обработващи лични данни
  - Срокове за съхранение на лични данни
  - Организационни и технически мерки за осигуряване на защита на данните.

„ДИЛЕКС“ ООД гарантира, че посочените дейности ще се преглеждат периодично, като част от общия одит на защитата на данните, и ще се извършва от ръководните органи на дружеството.

Заключителна разпоредба

§1. Настоящата Политика е приета от Общото събрание на „ДИЛЕКС“ ООД с Протокол от 20.12.2018 г.