Политика за спазване изискванията за защита на личните данни в Контракс АД

1. **Цел**

Целта на настоящата политика е осигуряване на контрол върху събирането, обработката и съхранението на информация съдържаща лични данни на субекти.

2. **Обхват**

Политиката е приложима за специфични среди, работещи и/или изискващи за прякото изпълнение на конкретни дейности лична информация на субект/и.

3. **Описание на дейностите**

Използването на лична информация за служителите, клиентите и контрагентите, както и начина на тяхната обработка, са неразделна част от дейността на „КОНТРАКС" АД. Дружеството е вложило значителни човешки, материални и финансови ресурси за изграждането на система за събиране, обработка и архивиране на личните данни.

Прилагането на настоящите изисквания има за цел:

- Защита на личните данни.
- Начина на обработка на личните данни като конфиденциалност, цялост и наличност.
- Ограничаване на риска за дейността и законността.
- Опазване доброто име на Дружеството.
- Изпълнение на договорните задължения.

Защитата на личната информация и данни, съхранявани и обработвани в „КОНТРАКС" АД е гарантирана, както се изисква от Закона за защита на личните данни, други нормативни разпоредби и/ или клаузи по договори.

Защита на личните данни се осъществява според приетите политики за защита на информацията . Тези указания са разпространени до всички лица, участващи в обработката на личната информация. Документите, съдържащи лични данни се индексират „за служебно ползване" според политиката за „ Категоризиране на Информацията" и се съхраняват от ООЧР.

За спазване на изискванията за получаване, обработка и съхранение на лични данни, приети като такива чрез заповед на Изпълнителния Директор, е определен за „ Служител по защитата на личните данни".

Определяне на „лични данни" :

Фирма Контракс АД определя категории лични данни и категории лица, който ще се обработват

Служители:

- Имена;

- ЕГН;
- Адрес;
- Телефон;
- Адрес на електронна поща;
- данни по лична карта и/или паспортни данни;
- свидетелство за съдимост
- медицинско свидетелство.
- образование и квалификация
- заплащане
- трудов стаж
- професионален опит
- здравно състояние

Клиенти - Физически лица
- Имена;
- ЕГН;
- Адрес;
- Телефон;
- Адрес на електронна поща;

Клиенти - Юридически лица
- Имена;
- ЕГН;
- Адрес;
- Телефон;
- Адрес на електронна поща;

Кандидати за работа:

Извършва се проучване на автобиографията на всички кандидати за работа, контрагенти и трети лица в съответствие с действащите закони, разпоредби и етика. То е пропорционално на бизнес изискванията, класифицирането на информацията и преценените рискове.

При проучването се спазват всички разпоредби на действащите закони: ЗЗЛД и трудовото законодателство.

Проверява се и се прилага за по-нататъшна обработка:

- проверка на автобиографията на кандидата (за пълнота и точност);
- потвърждение за заявени академични и професионални квалификации, ако това е възможно;
- независима проверка на самоличността (паспорт или друг подобен документ);
- кандидатите преминават през тест за ниво на професионална подготовка;
- интервю с контролни въпроси по предоставената информация в автобиографията, професионалната квалификация и др.

Когато длъжността при постъпване или при повишение включва достъп до средства за обработка на информация и ако на тях се обработва конфиденциална информация, по решение на ръководството се извършва по-подробна проверка за пълнота и точност на представените от кандидата за работа данни.

Когато се предвижда служителят да има достъп до класифицирана информация, се прилагат изискванията на ЗЗКИ.

Когато кандидатите за работа се набират чрез специализирана агенция, в договора с нея ясно се посочва отговорността й да извършва адекватна проверка на съобщаваните данни, проучване и за процедурите за уведомяване, които трябва да спазва както и начина за предоставяне на информация за личните данни на субекта съобразен с изискванията за защита на личните данни.

Информацията за всички избрани кандидати се събира, съхранява и обработва в „КОНТРАКС" АД при спазване из изискванията на ЗЗЛД.

Информация с лични данни на не одобрените кандидати за работа не се съхранява.

4. Цели за събиране на личните данни на субекти

Контракс АД определя конкретните цели за събиране, съхранение и обработка на личните данни както следва :

- трудови отношения,
- счетоводство,
- клиенти,
- доставчици,
- реклама и маркетинг
- законово определени цели

5.1 Контракс АД като администратор на лични данни:

Съхранението на събраните лични данни се осъществява чрез специализиран софтуер – Аладин, за период определен със заповед на Изпълнителния Директор, а именно:

1. За целия трудово-правен отношение за целия период като служител на Контракс АД. Съхранява се чрез специализиран софтуер – Аладин. Достъп до информацията има само отдел ТРЗ.
2. За 10 години след прекратяване на трудово-правно отношение. Заличава се информация за трите имена, дата на раждане, адрес, трудов стаж на бившия служител, предоставена банкова сметка, номер на застраховка.
3. За 50 години след прекратяване на трудово-правно отношение – съхранява се информация за заплати според Закона за счетоводството, член 12, ал.1. Използван софтуер за съхранение - Аладин.
4. Лични данни събрани при изпълнение на договор не се използват за маркетингови цели, ако изрично това не е упоменато в договора и не е получено съгласие от собственика на личните данни.

5.2 Контракс АД като обработващ лични данни

Лична информация за клиенти и контрагенти на Контракс АД се събират с цел договорни отношения или маркетинг.
Информацията за клиенти/ партньори се съхранява за период валидността на договора, след което се архивират в специализиран софтуер ERP система - Pantheon. Достъп до нея има Висшето ръководство и отдел Търговски.
Информация за маркетингови цели се събира и съхранява след предварително съгласие (чрез web site на Контракс АД, ел. поща или друг доказуем път) на отсрещната страна

поместена отново в специализирания софтуер – ERP Pantheon. Достъп до нея имат служители от отделите – Маркетинг, Търговски и Пред продажбена подготовка.
Информация за клиенти в сферата на здравеопазването – лични лекари – две имена, телефон, електронна поща и ЕИК, се събира и обработва чрез специализиран софтуер – Лиман. Достъпът до тази информация е ограничен до отдел Развойна дейност, поддръжка на Хипократ.
Лични данни на служители, контрагенти и доставчици се обработван само от Контракс АД.
Заявки за промяна; изискуема информация и заличаване се подават чрез приложени форми за искане на информация, промяна на информация и оттегляна на предоставена информация от собственика на лични данни; както и форми за уведомяване при нарушение на сигурността на личните данни – до собственика на личните данни и до контролния орган (КЗЛД). Контракс АД предоставя информация на субекта на лични данни със съдържание, определено от категориите за обработка в срок не по-късно от 7 работни дни за служители и до 14 работни дни за контрагенти и клиенти от дата на получаване на заявка за искане на информация.
Обработваните лични данни не се прехвърлят на трети лица или други държави, било то членки на Европейския съюз, без изричното упоменаване в договор/анекс към договор и получено съгласие от собственика на лични данни, с посочена причина за прехвърлянето, времето за обработка от трета страна и начина на съхранение и унищожаване на обработваните данни. Контролът за защита на прехвърлените лични данни е на организацията, поемаща отговорността за обработка.
Редът за подаване на заявки за промяна; изискуема информация и за заличаване на лични данни прехвърлени на трета страна се описват в договора/анекс към договор.

5. Предоставяна или разкриване на лични данни извън организацията

Естеството на работа на фирма Контракс АД е тясно свързана с предоставяне на чувствителна информация в това число и информация за личните данни на субекти и/или получаване на такава от субекти. Със заповед на ръководството и съобразно регулаторните изисквания към фирми регистрирани в Република България се определят следните основни направления:

- на публични органи:
    - Национална агенция за приходите – трите имена. ЕГН, длъжност, заплата и дата на договор.
    - Национален осигурителен институт- трите имена. ЕГН, длъжност, заплата и дата на договор.
    - Министерство на вътрешните работи - трите имена. ЕГН, длъжност.
    - Съдебни органи, ЧСИ - трите имена. ЕГН, длъжност
    - Застрахователи - трите имена. ЕГН, длъжност
    - Трудова медицина - трите имена. ЕГН, длъжност
- на обработващ лични данни
    - физическо лице, което обработва личните данни от името на администратора и по негово нареждане или възлагане - трите имена. ЕГН, длъжност, електронна поща.

- IT компания поддържаща приложен софтуер - трите имена, длъжност, електронна поща.

- на бизнес партньори
  - за целите на директен маркетинг - две имена, длъжност, електронна поща, физически адрес на организацията
  - съвместни продукти и услуги - две имена, длъжност, електронна поща, физически адрес на организацията

След получаване на съгласие от субекта на лични данни за тяхната обработка, Контракс АД няма да информира субекта/субектите на лични данни за работните им обмени.

За получено искане за разкритие на личните данни от трета страна, не упомената в списъка или в допълнително споразумение към трудов договор, или в анекса към договор с клиент, Контракс АД известява лично собственика на личните данни и причината за този иск, ако е упомената.

За промени в горепосоченият списък за обмен на информация, съдържаща лични данни с трети страни, както и правната и законова причина за тази промяна Контракс АД ще информира субектите на лични данни чрез писмо със свободен текст, но няма да изисква ново съгласие за обработка на личните данни от субекта за извършване на промяната.

6. Съхранение на личните данни в организацията

7.1 Срок:

Срокът за съхранение на личните данни е различен за различните дейности:

- за данните свързани с работните заплати, съгласно закона за счетоводството се съхраняват 50 години
- за данните свързани с клиенти, контрагенти и счетоводни записи за тях, съгласно закона за счетоводство се съхраняват до периода на последна данъчна проверка, но не по-малко от 6 години
- за данни свързани и получени при изпълнение на проект, срокът за съхранение се определя в подписания договор или в анекс към договора, но не по-дълъг от края на проекта.
- За данните свързани с видеонаблюдение, съгласно закона за защита на лични данни до 30 дни, с изключение на случаите, в които даден запис може да се явява доказателствен материал пред съда.
- Данни на потребители и техните клиенти на “Hipokrat - Cloud“ се съхраняват за законово определения за целите срок.

Срокът за съхранение на личните данни не се допуска да е по-дълъг от по-горе упоменатите срокове.

7.2 Обработка и защита на данните:

Според естеството на приложение и използване събраните лични данни във фирма Контракс АД се обработват както следва:

Досиета на служители:

- на хартиен носител – досие на служителя
- автоматизирано

Досиета на кандидати за работа:
- автоматизирано

Информация за клиенти :
- на хартиен носител – подписан договор
- автоматизирано

Информация за клиенти – маркетингови цели
- автоматизирано

Информация за партньори
- на хартиен носител – подписан договор
- автоматизирано

Контракс АД обработва лични данни чрез софтуерни продукти, което намаляват до минимум вероятността за неточностите в личната информация, която обработват.
За верността на самата информация отговаря собственикът на лични данни, както и остава негово задължение да информира Контракс АД за настъпили промени.
В случай на открита неточност в предоставената информация, служителят, обработващ личните данни своевременно информира собственика чрез налична форма – уведомление.
В случай, че неточността е в следствие на техническа грешка или проблем, се информира Длъжностното лице по защита н личните данни, завежда се като инцидент по информационна сигурност и се пристъпва към неговото разрешаване. Своевременно се информира и собственика на лични данни за настъпилия инцидент.
Когато инцидентът по сигурността е свързан със загуба или компрометиране на личните данни, Длъжностното лице уведомява контролния орган КЗЛД в рамките на 72 часа чрез налична форма за уведомление.
Проследяване за верността на данните и тяхната защита се осъществява през целия им жизнен цикъл

7.2.1 Работни процеси свързани с обработката на лични данни

Отдел „Труд и работна заплата“ – използва се специализиран софтуер „АЛАДИН“ за обработка на лична информация на служителите. Фирма Контракс АД има подписан договор за поддръжка и настройки на програмата според текущата необходимост.
За защита на информацията, обхващаща и раздел лични данни са приложени криптиращи механизми.

Отдел „ Сервиз“ , отдел „ Търговски“ – използва се специализиран софтуер ERP система – „Пантеон“. Достъпът до тази система се основава на политика „ Политика за контрол на достъпа“ на фирма КОНТРАКС с регламент и процес описан и управляван в прилежащите политики съгласно стандарта ISO 27001:2013.

7.2.2 Изисквания за съхранение и обработка на личните данни към работната станция на служител „Труд и работна заплата“:

Работната станция се съхранява в контролирани условия извън обсега на външни лица, а когато не се ползва, се заключва в определени за целта сигурни зони.
Информационните носители се пазят от възможни поражения на обкръжението като силна топлина, директна слънчева светлина и източници на магнитни полета.
Избягват се заплахите от обкръжението за хардуера като храна, дим, течности или влажност, рязко загряване или охлаждане.

Служителят, обработващ лични данни, не се допуска да работа на промененото оборудване, преди то да бъде проверено и предадено за експлоатация. Това не се отнася за временни премествания на преносимите компютри, чиито основни връзки са били инсталирани от отдел „Сервиз информационни технологии".
Служителят е обучен, как да опази зачисленото му електронно оборудване и информацията в него.

7.2.3 Изисквания за съхранение и обработка на личните данни към сървър с

ЕРП система Pantheon:

Достъпът до информация или информационни системи се основава на изискванията на бизнеса и изискванията за сигурност (според ISO/IEC 27001:2013), залегнали в „Политика по информационна сигурност" и „Политика за управление на пароли".
В настоящата политика се прилага правилото - „Всичко, което не е изрично разрешено, е забранено!".

ТРЗ система Аладин:

Достъпът до информация или информационни системи се основава на изискванията на бизнеса и изискванията за сигурност (според ISO/IEC 27001:2013), залегнали в „Политика по информационна сигурност" и „Политика за управление на пароли".
В настоящата политика се прилага правилото - „Всичко, което не е изрично разрешено, е забранено!". Системата се намира на строго определен компютър, защитен от мрежови достъп. Достъпът до данните в системата се осъществява само от служителя, отговарящ за ТРЗ или негов заместник обявен със заповед на Изпълнителния директор на Контракс АД.

7.2.4 Изисквания за съхранение на лични данни на хартиен носител

Съхранението на лични данни (досиета на служители, досиета на кандидати за работа) се осъществява при строго регламентиран ред в отдел ТРЗ. Данните са категоризирани, приложени в съответните папки и заключени в шкаф със специално предназначение.
Сигурността на мястото за съхранение е регламентирана в „Политика за физическа сигурност".

Съхранението на договори, анекси към тях и протоколи се извършва съгласно процедурите изпълнявани според изискванията на стандарта за управление на качеството ISO 9001.
Пълна информация се съхранява в ERP системата – Pantheon. Достъп до нея има висшето ръководство и отдел Търговски.

7.2.5 Защита на личните данни

При обработка на личните данни, Контракс АД ги защитава чрез използването на криптиращи механизми и електронни сертификати. Контракс АД не прилага други механизми за „прикриване" / минимизиране на личните данни.

7.2.6 Физическа сигурност и трансфер на лични данни

Политика на „КОНТРАКС" АД е да се предпазват компютърния хардуер, софтуер, данните и документацията от загуби, кражби, неупълномощен достъп и поражения от околната среда.
Физическият достъп до помещения на фирмата е регламентиран със заповед на управителя.
Правата на достъп кореспондират с изискванията на „Политика за оценка на съответствието", т.е. да не противоречат на законови и нормативни изисквания.
Съобразно изискванията за физическа защита на личните данни и на местата за тяхното съхраняване е заведена „Политика за физическа сигурност", където по-специално е обърнато внимание на

- Достъпът до помещенията, в които е разположено критичното за дейността на фирмата оборудване.
- Забрана за съхраняването на архивирани материали на резервни носители
- Забрана за съхранението на опасни вещества (лесно запалими материали или агресивни химикали) вътре или в близост до сървърното помещение и места за съхранение на лични данни7.
- Забрана за влизането с фотографски, видео- , аудио- или други записващи устройства вътре в специалните зони, освен ако не е дадено специално разрешение.
- Използването на адекватна по предназначение и капацитет пожаро известителна техника, видео наблюдение и СОТ

Пренос/трансфер на информация съдържаща лични данни се осъществява чрез криптирани, защитени връзки с приемчика на тази информация. Ако изграждането на такъв тунел не е възможно, преносът се осъществява чрез куриер на Контракс АД, преминал специално обучение.

7. Унищожаване/заличаване на лични данни

Личните данни в ТРЗ не подлежат на унищожаване съгласно закона за счетоводство член 12, ал 1 за период от 50 години.

Личните данни в счетоводната програма, касаещи контрагенти, подлежат на архивиране и срок за съхранение от 10 години според закона за счетоводство чл. 12, ал. 1.след този период, данните могат да бъдат изтрити, а личните данни заличени.

Лични данни, предоставени във връзка с изпълнение на договор се унищожават автоматично след приключването на договора чрез изтриване, ако в договора/анекс към договора не е посочено друго.

Лични данни на пациенти, чийто лични лекари използват приложен софтуер „Хипократ-Нео" могат да бъдат унищожени след изтичане на срока за съхранение:

- на медицински досиета, зададен в Закона за здравето изм., бр. 24 от 22.03.2019 г., в сила от 1.01.2020 г – носители на ТЕЛК и НЕЛК – 40 години след последното издаване. За всички останали – след 5 години.
- Закон за здравето, чл. 132, ал. 3 – ЛЗ по чл.131, ал.1, т.2 от ЗЗ (СИМП с разрешение за извършване на дейности по асистирана репродукция) съхраняват информацията 30 години.

Наредба №39/16.11.2004г. за профилактичните прегледи и диспансеризацията

- чл. 9, ал. 1 - Лечебните заведения съхраняват медицинската документация за извършените от тях профилактични прегледи и изследвания три години

- чл. 9, ал. 2 - Личният лекар съхранява медицинската документация за всички извършени профилактични прегледи и изследвания на пациентите, включително извършени и от други лечебни заведения, три години след навършване на 18-годишна възраст - за децата, а при бременните - три години след прекратяване на бременността.

- Болнични листове – Чл. 54, ал. 4 от Наредба за медицинската експертиза – Анулираните листове се съхраняват 3 години след датата на издаването им.

- Зелени и жълти рецепти – срок на съхранение 1 година съгласно Чл. 12, ал. 1 от НАРЕДБА № 4/04.03.2009 Г. ЗА УСЛОВИЯТА И РЕДА ЗА ПРЕДПИСВАНЕ И ОТПУСКАНЕ НА ЛЕКАРСТВЕНИ ПРОДУКТИ

Лични данни на практикуващи лекари се променят/изтриват след подаване на форма за искане на субекта на данни и данните ще бъдат обработени по надлежен начин.

Лична информация предоставена в хартиен вид подлежи на унищожение чрез шредер, след изтичане на срока за нейното съхранение или срока на целта, за която е била събирана.

8. Нарушения

Неспазването на водещите принципи на настоящата Политика, може да доведе до дисциплинарни действия от страна на „КОНТРАКС" АД, в зависимост от вида и тежестта на нарушението, особено ако то предизвика нестабилност или загуби за Дружеството и/или представлява повтарящо се нарушение.
В анекс към договор за защита на личните данни / споразумение за защита на личните данни (доставчици) индивидуално се дефинират действията, които страните биха предприели при открити нарушения със сигурността и компрометиране на личната информация.

9. Права на субектите на данни

Според европейски регламент (ЕС) 2016/279 всеки субект на лични данни има права, предвидени в регламента. Фирма Контракс АД стриктно спазва тези изисквания и ги прилага както следва:

- Право на информация към момента на събиране на данните – член 13 и член 14 – субектите на данни имат право да им бъде предоставена информация от администраторите на лични данни още в момента, в който последните съберат / получат личните данни, а по-конкретно:
  фирма Контракс АД,
  е-мейл: dpo@kontrax .bg

Правото на информация за лични данни се дава само на лицето, носител на тези данни както следва:

Име, бащино, фамилно, ЕГН, адрес по лична карта, телефон – личен/ служебен, банкова сметка, застрахователна полица. Цел за искане на информация – настъпили промени и изменения.

Информация за лични данни изискана от трето лице, не споменато в политиката, не се предоставя.

- Право на достъп – член 15 – Контракс АД ще предостави изискуемата от субекта информация за обработка на личните данни , само ако е направено запитване според установения ред и в регламентирания времеви период.
- Право на коригиране – член 16 - Субектът на лични данни може да поиска коригиране на същите, в случай че открие неточности, както и допълване на липсваща информация.

- Право на изтриване (право да бъде забравен) – член 17 – фирма Контракс АД приема възможността личните данни да бъдат изтрити в следните случаи:
    - личните данни повече не са необходими за целите, за които са били събрани или обработвани по друг начин;
    - субектът на данните възразява срещу обработването;
    - личните данни са били обработвани незаконосъобразно;
- Право на ограничаване на обработването – член 18 – при установена неточност или неправомерност в обработката на лични данни, и при възражение от страна на субекта за обработка на личните му данни.

- Право на възражение – член 21 - фирма Контракс АД ще прекрати обработването на личните данни както следва:
    - при възражение от страна на субекта, 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.
    - при възражение срещу обработване за целите на директния маркетинг,
    - при възражение към приложени научни изследвания или за статистически цели, освен ако обработването е необходимо за изпълнението на задача, осъществявана по причини от публичен интерес.
- Право на жалба до надзорен орган – член 77 – всеки един субект на лични данни има право да подаде жалба към надзорния орган - КЗЛД в Република България, ако счита че обработката на лични данни отнасящи се до него, нарушава разпоредбите на регламент ЕС 2016/679 и закона за защита на личните данни.

- Ограничение на предоставените права – член 23 са свързани с ограниченията съгласно закона за ТРЗ и закона за счетоводството – субектът на лични данни не може да изисква изтриване на информация, свързана с тях.

10. Съгласие

С цел изпълнение на политиките на фирма Контракс, свързани с конкретни нейни действия, всеки един субект на лични данни трябва да подпише декларация, с която да даде писменото си съгласие за обработка и съхранение на личните му данни.

Регистри

В Контракс АД се поддържат следните регистри:

Регистър на дейностите по обработване (на администратора) - чл. 30, пар. 1 от ОРЗД
Регистър на дейностите по обработване (на обработващия) - чл. 30, пар. 2 от ОРЗД
Регистър на исканията от субектите на данни
Регистър на нарушенията

11. Длъжностно лице по защита на данните

Връзка с отговорното лице по защита на данните в Контракс АД е осъществима чрез dpo@kontrax.bg.