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

Разработил	Проверил	Утвърдил
Инж. Б. Николова	инж. Я. Пилософ,	инж. Й. Йорданов, ИД

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. Определение

лични данни – всяка информация, свързана с идентифицирането на физическото лице или физическите лица, което може да бъде идентифицирано пряко или непряко чрез идентификатор като име; идентификационен номер; данни за местонахождение; онлайн идентификатор; физическа, физиологическа, генетична, психическа, умствена, икономическа, културна или социална идентичност на това физическо лице.

обработване – всяка операция или съвкупност от операции, извършвана с личните 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 ограничаване, изтриване или унищожаване.

ограничаване на обработването - маркиране на съхранявани лични данни с цел ограничаване на обработването им в бъдеще.

администратор - 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.

получател - физическо или юридическо лице, публичен орган, агенция или друга структура, пред която се разкриват личните данни, независимо дали е трета страна или не.

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.

съгласие на субекта на данните - 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.

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;

4. Описание на дейностите (Задължения и роли по Регламент (ЕС) 2016/679)

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. Документите, съдържащи лични данни се индексират „за служебно

ползване” според политиката за „ Категоризиране на Информацията“ – ПИС 19 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“ г-н Яко Пилософ.

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 - Юредически 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 неодобрените кандидати за работа не се съхранява.

5. 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 – Аладни. 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.

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 на отсрещната страна поместена отново в специализирания софтуер – ERP Pantheon. Достъп до нея имат служители от отделите – Маркетинг, Търговски и Предпродажбена 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.

6. 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.
  - счетоводна къща - 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

7. 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 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.

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

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 ЕРП система – „Пантеон“. Достъпът до тази система се основава на политика „ Политика за контрол на достъпа“ – ПИС 11 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 трябва да се съхранява в контролирани условия извън обсега на външни лица, а когато не се ползва, трябва да се заключва в определени за целта сигурни зони.
Информационния носител да се пазят от възможни поражения на обкръжението като силна топлина, директна слънчева светлина и източници на магнитни полета.
Трябва да се избягват заплахите от обкръжението за хардуера като храна, дим, течности или влажност, рязко загряване или охлаждане.

Служителят, обработващ лични данни, да не се допускат 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 трябва да бъде 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 ПИС 01 Политика по информационна сигурност и ПИС 04 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 ПИС 01 Политика по информационна сигурност и ПИС 04 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 ПИС 9 - 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 Физическа сигурност

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 ПИС 15 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 – ПИС 9“ 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

8. Унищожаване 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 съхранение в рок от 10 години.

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.

9. 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.

10. 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,
  отговорно лице – Яко Пилософ
  е-мейл: office@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 (Обн., ДВ, бр. 1 от 4.01.2002; с изменение в сила от 1.01.2018 г., изм., бр. 7 от 19.01.2018 г.)

- 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.

11. 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. Декларацията е представена като Приложение 1 към тази политика.

12. 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

13. Длъжностно лице по защита на данните

Отговорно лице по защита на личните данни в Контракс АД е г-н Яко Пилософ. В своята дейност той ще бъде подпомаган от Бистра Николова, водещ одитор по ISO 27001 и ISO 20000-1 и Румяна Йолова, водещ одитор по ISO 9001, ISO 14001 и OHSAS 18001.