ОБЩА ПОЛИТИКА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ
на Кооперация Китка
Дата 22.05.2018

ВЪВЕДЕНИЕ

Ние от Кооперация Китка считаме гарантирането на правото на защита на личните данни за наш основен ангажимент, поради което ще използваме и вложим всички необходими средства и усилия, за да обработваме Вашите данни при пълно съответствие с Регламент (ЕС) 2016/679 („Общият регламент на ЕС относно защитата на данните“ или „ОРЗД“) и всяко друго приложимо законодателство. Тъй като един от основните принципи на тази правна рамка е прозрачността, ние сме изготвили настоящия документ, чрез който искаме да ви уведомим за начина, по който събираме, използваме, предаваме и защитаваме Вашите лични данни.
Запазваме си правото периодично да актуализираме и изменяме настоящата Политика, за да отразяваме всички изменения на начина, по който обработваме личните Ви данни или измененията на законовите изисквания. В случай на такива изменения, ние публикуваме изменената версия на Политиката на нашия уебсайт и поради това, любезно ви молим периодично да проверявате съдържанието ѝ.

ОБХВАТ

Материален и териториален. ОРЗД се прилага за обработването на лични данни изцяло или частично с автоматични средства, както и за обработването с други средства, на лични данни, които са част от регистър с лични данни или които са предназначени да съставляват част от регистър с лични данни. Правилата на ОРЗД са в сила спрямо обработването на лични данни в контекста на дейностите на дадено място на установяване на администратор или обработващ данни в Съюза, независимо дали обработването се извършва в Съюза или не. Регламента се прилага за обработването на лични данни на субекти на данни, които се намират в Съюза, от администратор или обработващ, който не е установен в Съюза, когато става въпрос за предлагане на стоки или услуги на такива субекти на данни в Съюза и наблюдение на тяхното поведение, доколкото това поведение се проявява в рамките на Съюза.
Политиката обхваща използването и обработването на лични данни за всички лица, включително клиенти, служители, изпълнители и доставчици. Всеки в кооперацията следва да спазва настоящата политика при обработката на лични данни. Не съществуват изключения от това правило.

ДЕФИНИЦИИ

За целите на настоящата политика долупосочените термини имат следното значение: „Администратор" - всяко физическо или юридическо лице, публичен орган, агенция или друга структура, която сама или съвместно с други определя целите и средствата за обработването на лични данни; когато целите и средствата за това обработване се определят от правото на ЕС или правото на държава членка, администраторът или специалните критерии за неговото определяне могат да бъдат установени в правото на Съюза или в правото на държава членка. Кооперация Китка е администратор на лични данни.

„Обработващ лични данни“ е всяко лице, което обработва Лични данни от името на Администратор на лични данни. Служителите на Администраторите на лични данни са изключени от обхвата на това определение, но доставчиците, които обработват Лични данни от име на Китка, се включват в обхвата.
„Субект на данни“ е идентифицирано физическо лице, за което се отнасят Лични данни или физическо лице, което може да бъде идентифицирано и до което се отнасят Лични данни. За целите на тази политика субектите на данни могат да бъдат служители, клиенти и/или представители на доставчици и бизнес партньори, както и други физически лица, чиито Лични данни могат да бъдат обработвани от Администратора.
„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" - означава всяка операция или съвкупност от операции, извършвана с лични данни или набор от лични данни чрез автоматични или други средства като събиране, записване, организиране, структуриране, съхранение, адаптиране или промяна, извличане, консултиране, употреба, разкриване чрез предаване, разпространяване или друг начин, по който данните стават достъпни, подреждане или комбиниране, ограничаване, изтриване или унищожаване;
„Специални категории лични данни“ – лични данни, разкриващи расов или етнически произход, политически възгледи, религиозни или философски убеждения, или членство в синдикални организации и обработката на генетични данни, биометричните данни за уникално идентифициране на физическо лице, данни отнасящи се до здравето или данни относно сексуалния живот на физическо лице или сексуална ориентация.
„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;
„Дете“ –Обработката на лични данни на едно дете е законно само, ако родител или попечител е дал съгласие. Администраторът полага разумни усилия, за да провери в такива случаи, че притежателят на родителската отговорност за детето е дал или упълномощен да даде съгласието си.
„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, и по-конкретно за анализиране или прогнозиране на аспекти, отнасящи се до изпълнението на професионалните задължения на това физическо лице, неговото икономическо състояние, здраве, лични предпочитания, интереси, надеждност, поведение, местоположение или движение;
„Нарушение на сигурността на лични данни" - нарушение на сигурността, което води до случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или достъп до лични данни, които се предават, съхраняват или обработват по друг начин;
„Получател" - физическо или юридическо лице, публичен орган, агенция или друга структура, пред която се разкриват личните данни, независимо дали е трета страна или не. Същевременно публичните органи, които могат да получават лични данни в рамките на конкретно разследване в съответствие с правото на Съюза или правото на държава членка, не се считат за „получатели"; обработването на тези данни от посочените

публични органи отговаря на приложимите правила за защита на данните съобразно целите на обработването;
„Трета страна“ – всяко физическо или юридическо лице, публичен орган, агенция или друг орган, различен от субекта на данните, администратора, обработващия лични данни и лицата, които под прякото ръководство на администратора или на обработващия лични данни имат право да обработват личните данни;

ВИДОВЕ ЛИЧНИ ДАННИ, ОБРАБОТВАНИ В КИТКА

Китка събира лични данни във връзка със следните категории данни (изброяването е неизчерпателно):
- данни на кандидати за работа и персонал на кооперацията, свързани с тяхната (потенциална) позиция в Китка(включително данни за контакт, автобиография и други);
- данни за зависимите от служители на Китка лица, както и за членовете на семейството на служителите на кооперацията, във връзка с целите на осигурителното и данъчното законодателство;
- клиентите ни и потенциалните ни клиенти, свързани с продуктите и услугите, които предлагаме; търговските партньори на Китка, както и други лица, отговарящи за управлението на търговските взаимоотношения;
В определени и ограничени случаи Китка може да обработва и специални категории лични данни, особено за служителите си, на основание на законодателството на страната.

ЗАДЪЛЖЕНИЯ НА КООПЕРАЦИЯ КИТКА ВЪВ ВРЪЗКА СЪС ЗАЩИТАТА НА ЛИЧНИ ДАННИ

Китка има следните задължения в качеството си на администратор на лични данни:
- определя политиката за защита на личните данни в кооперацията, спазва изискванията на ОРЗД и националното законодателство;
- извършва анализ от нуждата за длъжностно лице по защита на данните и назначава такова, ако е приложимо;
- осигурява организацията по водене на регистрите на дейностите, свързани с обработване на лични данни, съгласно предвидените мерки за гарантиране на адекватна защита;
- въвежда, както към момента на определянето на средствата за обработване, така и към момента на самото обработване, подходящи технически и организационни мерки, които са разработени с оглед на ефективното прилагане на принципите за защита на данните;
- осигурява упражняването на правата на физическите лица за защита на личните данни;
- въвежда подходящи технически и организационни мерки, за да гарантира и да е в състояние да докаже, че обработването на лични данни се извършва съобразно изискванията на ОРЗД;
- въвежда 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;
- осъществява контрол по спазване на изискванията за защита на регистрите, установява обстоятелства, свързани с нарушаване на тяхната защита, и предприема мерки за тяхното отстраняване;
- актуализира поддържаните регистри с лични данни;

- поддържа личните данни във вид, който позволява идентифициране на съответните физически лица за период не по-дълъг от необходимия за целите, за които тези данни се обработват;
- периодично информира и обучава персонала по въпросите на защитата на личните данни;
- оказва съдействие при осъществяването на контролните функции на Надзорния орган (за България - Комисия за защита на личните данни), подпомага установяването на обстоятелства, свързани със защитата на личните данни;
- определя правата на служителите за достъп до лични данни в информационните системи съобразно целите на обработване, така че да се гарантира законосъобразност и да се спазят принципите на обработване;
- използва само обработващи лични данни, които предоставят достатъчни гаранции посредством прилагането на подходящи технически и организационни мерки за защита;
- в случай на нарушение на сигурността на личните данни, уведомява, надзорния орган по защита на личните данни без ненужно забавяне при установен риск за засегнатите лица, не по-късно от 72 часа след като е разбрал за него. Надзорният орган не се уведомява когато не съществува вероятност нарушението на сигурността на личните данни да породи риск за правата и свободите на физическите лица;
- в случай на установен висок риск за физическите лица, ги информира по подходящ начин за нарушението по сигурността на личните данни;
- 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;
- извършва оценка на въздействието съгласно изискванията на чл. 35 от регламента.

ПРИНЦИПИ НА ЗАЩИТА НА ДАННИТЕ

Придържането към принципите, поставени като изискване от ОРЗД, е от основно значение за подпомагане на практическото прилагане на регламента и за демонстриране на отговорно отношение. Лични данни могат да бъдат обработвани само в съответствие с настоящата Политика и следвайки принципите, както са описани по-долу:

1. Законосъобразност, добросъвестност и прозрачност

Всеки път, когато лични данни биват събирани, те трябва да се събират с яснота относно законната бизнес цел, с оглед осъществяването на която данните се събират. Обработването на лични данни трябва да е въз основа на едно от правните основания за обработване, описани в регламента, в противен случай няма да е законосъобразно.

Развитието, практиките и политиките по отношение на личните данни следва да бъдат създавани и актуализирани в съответствие с основния принцип на откритост. Кооперацията е длъжна да предоставя информация и да съдейства на лицата, които желаят да разберат дали и как се обработват личните им данни, както и данните за администратора, който ги обработва.

2. Ограничение на целите

Данните се събират за конкретни, изрично указани и легитимни цели и не се обработват по-нататък по начин, несъвместим с тези цели.

2. Свеждане на данните до минимум

Всяко събиране на лични данни трябва да бъде ограничено до данните, необходими за целта, за която администратора ги е събрал. Личните данни трябва да се получават само по законосъобразни и прозрачни начини и когато е уместно, със знанието или съгласието на физическото лице, за което се отнасят данните, без съгласието да е единствено и абсолютно основание за обработване на лични данни.

Когато е възможно, Личните данни трябва да бъдат анонимизирани, псевдонимизирани или обобщени в максимална степен.

4. Точност

Личните данни трябва да бъдат точни, пълни, събрани с оглед целта на обработката им и поддържани актуални. Следва да бъде дадена възможност на субектите на данни да актуализират собствените си данни, а ако това не е приложимо, да се въведат процеси, които да гарантират точността на данните

5. Ограничение на съхранението

Личните данни трябва да се съхраняват във форма, която позволява идентифицирането на субекта на данните за период, не по-дълъг от необходимото за целите, за които се обработват личните данни.

6.Цялостност и поверителност

Личните данни се обработват по начин, който гарантира подходящо ниво на сигурност, включително срещу неразрешено или незаконосъобразно обработване и срещу случайна загуба, унищожаване или повреждане, като се прилагат подходящи технически или организационни мерки. Запазването на сигурността и защитата на лични данни е от изключително значение при всяко обработване.

Китка следва да разработва процедури за сигурността и целостта на личните данни и тези мерки да съответстват на нивото на риск за правата на субектите на данни.

При използване на лица, подизпълнители или доставчици Китка гарантира, че такива лица, имащи достъп до лични данни, също отговарят на изискванията за сигурност, техническите и организационни мерки за сигурност на кооперацията.

7. Отговорност, отчетност

Администраторът, който е събрал данните и определя как се обработват – трябва да бъде отговорен за спазването на мерките, разработени в резултат на прилагането на посочените по-горе принципи.

Принципът на отчетност означава, че Китка следва да може да демонстрира във всеки един момент съответствие с изискванията на ОРЗД. Това се постига чрез прилагане на следните практики:

- Съответствие с местното действащо законодателство и приложимото такова в зависимост от случая и прилагане на адекватни технологични и организационни мерки за защита на данните;
- Извършване на оценка на въздействие върху защита на данните по отношение на всяка нова дейност по обработване, която може да представлява висок риск за правата и свободите на физическите лица;
- Спазване на защита на данните на етапа на проектирането и по подразбиране при разработването на нови технологии, системи, приложения или бизнес процеси;
- Адекватно и периодично обучение на лицата за организационните и технически мерки за защита на данните, създаване на план за това обучение;
- Провеждане на редовни вътрешни и външни одити на практиките на кооперацията при обработване на личните данни;
- Навременно докладване на релевантните лица и органи при нарушения на защита на личните данни и постоянно анализиране на настъпилите нарушения с цел подобрение в процесите и системите на дейността на кооперацията;
- Съдействие при евентуално регулаторно разследване

Защита на данните на етапа на проектирането се отнася до подход към проекти, които осигуряват спазването на поверителността и защитата на данните от самото начало. При въвеждането на нови технологии, системи, приложения и/или процеси Китка трябва да приложи подходящи технически и организационни мерки, за да гарантира, че защитата на данните е основен фактор в ранните етапи на всеки проект, както и през жизнения му

цикъл. Оценката на въздействието върху защитата на данните е процес, който помага за оценката на рисковете за поверителността на данните при събирането, използването и разкриването на лична информация. Оценката на въздействието върху защитата на данните би могла да бъде подобрена от подходите за защита на данните на етапа на проектиране и по подразбиране.
Китка трябва да поддържа данните в идентифицируема форма само докато е необходимо за изпълнение на целите, за които данните се обработват. Всички останали данни следва да бъдат изтрити от всички системи и всички носители в кооперацията след установения период за съхранение, който е определен с оглед изискванията на местното законодателство и на бизнес дейността на фирмата. Постигането и преследването на легитимните интереси на кооперацията не следва да бъде в противоречие, а в баланс с правата на субектите на данни. Последното се постига като се създава специална политика за правата и начините за упражняването им, както и периодично актуализиране на политиката за съхранение на данни.
.
ПРАВА НА СУБЕКТИТЕ НА ДАННИ

Китка предприема необходимите мерки за предоставяне на информация на физическите лица относно обработването на лични данни в кратка, прозрачна, разбираема и лесно достъпна форма, на ясен и прост език. Администраторът съдейства за упражняването на правата на субекта на данните по членове 15-22 от ОРЗД, с изключение на случаите, когато не е в състояние да идентифицира физическото лице.
Субекта на данни има право на:
- Право на достъп: Право на искане на копие от Лични им данни, които се обработват от Китка и от трети лица, с които кооперацията работи (например доставчици на осигурителни и разплащателни услуги). Право на достъп до данните на физическото лице включва:
- целите на обработването;
- категориите лични данни;
- сроковете за съхранение на личните данни;
- съществуването на право на коригиране или изтриване на лични данни или ограничаване на обработването на лични данни, или възражение обработване; правото на жалба до Надзорен орган;
- източниците на лични данни;
- съществуването на автоматизирано вземане на решения, включително профилиране.
Съгласно правото на субектите на данни за достъп до данните им, дадено лице има право на информация, свързана само със собствените му лични данни, а не на информация, свързана с други хора, освен ако лицето, подаващо искането, действа от името на това лице.
- Право на поправяне: Правото на поправка на неточни или непълни лични данни.
- Право на изтриване: Правото на лични данни да бъдат окончателно премахнати, което означава, че вече не се обработват.
То се прилага само в следните конкретни ситуации:
- когато личните данни вече не са необходими за първоначалната цел, за която са били събрани/обработени;
- когато данните са незаконно обработени (т.е. по начин, който е в нарушение на ОРЗД);
- ако субектът на данните оттегли своето съгласие и няма друго правно основание (например законни интереси) за обработката на личните му данни.
Въпреки това, Китка може да запази личните данни, когато:
- съществуват убедителни основания (например неблагоприятни събития);

- данните са необходими, за да се спази правно задължение (например фирмени записи на данни, финанси, одит); или е необходимо за завеждане, водене или защита по правни искове (например задържане при висящ съдебен спор).
- Право на ограничаване на обработването: Правото да се изисква от Китка временно или постоянно да преустанови обработването на всички или някои от личните им данни. Ако данните са били разкрити на други лица, трябва да се уведомят за ограничаването на обработката на данните (освен ако това е невъзможно или води до несъразмерно усилия). Това право също има определени описани в ОРЗД случаи, в които е приложимо.
- Право на преносимост на данните: Правото да получават личните данни в структуриран, широко използван, машинно четаем и оперативно съвместим формат, като им се дава възможност да предоставят Личните си данни на друг администратор на лични данни сами или директно чрез фирмата. То се прилага само когато са налице всички изброени по-долу предпоставки:
1. личните данни се обработват по автоматизиран начин (т.е. няма записи на данните на хартиен носител);
2. личните данни са доброволно предоставени на администратора от субекта на данните; и
3. основанието за обработка е само съгласието на субекта на данните или ако данните се обработват с оглед изпълнението на договор или като подготвителни стъпки към сключването на договор.
- Право на възражение: Право на възражение срещу обработването на Личните данни, когато обработването се основава на съображения от обществен или законен интерес или се извършва за целите на директния маркетинг.
- Автоматизирано вземане на решения (включително профилиране): правото да не се вземат решения, основани единствено на автоматизирано индивидуално вземане на решения, включително профилиране, които имат правно действие по отношение на Субектите на данни или ги засягат значително.
- Право на даване, промяна или оттегляне на съгласие за обработване на лични данни за случаите, когато съгласието е основание за обработване на данните.
За да осигури механизъм и гаранция на правата на субектите на данни, Китка създава вътрешен процес за обработване и проследяване на искания на субекти на данни.

СЪГЛАСИЕ ЗА ОБРАБОТВАНЕ НА ДАННИ

На основание чл. 6(1) от ОРЗД съгласието от лицето е едно от допустимите условия за законосъобразност на обработването на лични данни. Съгласие следва да се дава лично чрез писмена декларация, в електронна форма или друг определен от Администратора начин, с който да се гарантира, че съгласието е:
- свободно дадено,
- конкретно,
- информирано и
- недвусмислено
от страна на физическото лице. Мълчаливото съгласие, предварително отметнатите полета или липсата на действие не следва да се считат за съгласие.
Китка следва да осигури възможност на лицата по лесен начин да променят или оттеглят съгласието си, без това да поражда неблагоприятни правни последици за тях.

СИГУРНОСТ НА ДАННИТЕ

Всички служители на кооперацията са инструктирани за процесите по обработка на лични данни и гарантират за тяхната сигурност. Китка въвежда вътрешни политики за обработка на данни, съгласно които достъп до данни имат само лица, които се нуждаят от тях при изпълнение на служебните си задължения.

ОТНОШЕНИЯ С ОБРАБОТВАЩИ ЛИЧНИ ДАННИ

При възлагане обработването на лични данни на трети страни Китка в качеството си на администраторът спазва следните изисквания:
- Избират се само обработващи, които предоставят достатъчни гаранции за прилагането на подходящи технически и организационни мерки за защита на личните данни.
- В писмените договори с обработващите се уреждат условията за защита на личните данни.
- Субектите на данни се информират по установения ред.

Договорите с Обработващите следва да съдържат най-малко следните реквизити:
- предмета и срока на действие на обработването;
- целите и естеството на обработването;
- категориите физически лица, за които се осъществява обработването;
- категориите лични данни, които са в обхвата на обработването;
- правата и задълженията на Администратора;
- Изисквания към Обработващия съгласно чл. 28 (3) от ОРЗД.

ПРЕДОСТАВЯНЕ НА ЛИЧНИ ДАННИ. ТРАНСФЕР

Прехвърляне на лични данни в трета страна или международна организация се извършва само при едно от следните условия:
- субектът на данните изрично се е съгласил с предложеното прехвърляне, след като е бил информиран за възможните рискове от такива прехвърляния;
- предаването е необходимо за изпълнението на договор между субекта на данните и администратора или за изпълнението на преддоговорни мерки, взети по искане на субекта на данните;
- предаването е необходимо за сключването или изпълнението на договор, сключен в интерес на субекта на данните между администратора и друго физическо или юридическо лице;
- предаването е необходимо поради важни причини от обществен интерес;
- предаването е необходимо за установяването, упражняването или защитата на правни претенции;

УПРАВЛЕНИЕ НА ИНЦИДЕНТИ ПРИ СИГУРНОСТТА

Управлението на инциденти по сигурността на личните данни се основава на изискванията в чл. 33 и чл. 34 от регламента. В случай на нарушение на сигурността, което може да породи висок риск за правата и свободите на лицата, Администраторът има 72-часов срок за информиране на Надзорния орган. При наличие на висок риск задължително се уведомяват и физическите лица.

Когато е налице висок риск и какъв е процесът за управление на инциденти в Китка, се описва в отделна процедура.

ИЗВЪРВАНЕ НА ОЦЕНКА НА ВЪЗДДЕЙСТВИЕТО ВЪРХУ ЗАЩИТА НА ДАННИТЕ

Оценката на въздействието върху защитата на данните се въвежда в чл. 35 от ОРЗД и представлява процес, чиято цел е да опише обработването, да оцени неговата необходимост и пропорционалност и да спомогне за управлението на рисковете за правата и свободите на физическите лица, произтичащи от обработването на лични данни, като ги оцени и определи мерки за справяне с тези рискове.
На основание чл. 35(1) от ОРЗД, когато съществува вероятност определен вид обработване, по-специално при което се използват нови технологии, и предвид естеството, обхвата, контекста и целите на обработването, да породи висок риск за правата и свободите на физическите лица, преди да бъде извършено обработването, администраторът извършва оценка на въздействието на предвидените операции по обработването върху защитата на личните данни. В една оценка може да бъде разгледан набор от сходни операции по обработване, които представляват сходни високи рискове.
Администраторът извършва оценка на въздействието върху защитата на данните съгласно специална приета вътрешна процедура за оценка на въздействието върху защитата на данните.

ТЕХНИЧЕСКИ И ОРГАНИЗАЦИОННИ МЕРКИ ЗА ЗАЩИТА НА ДАННИТЕ

Китка предвижда необходимите технически и организационни мерки за защита на личните данни от случайно или незаконно унищожаване, или от случайна загуба, от неправомерен достъп, изменение или разпространение, както и от други незаконни форми на обработване.
Видовете защита биват физическа, персонална, документална, защита на автоматизирани информационни системи и/или мрежи, криптографска защита.
Администраторът предприема следните мерки за защита на личните данни:

- мерки за физическа защита на личните данни, представляваща система от технически и организационни мерки за предотвратяване на нерегламентиран достъп до сгради, помещения и съоръжения, в които се обработват лични данни включват:
1. технически мерки:
- система за контрол на достъпа до помещенията на кооперацията;
- заключване на помещенията в извънработно време и регламентиране на достъпа до тях;
- осигуряване на заключващи се помещения и шкафовете за съхранение на информация, свързана с лични данни в предвидените от вътрешно-организационните и нормативни документи случаи;
- оборудване на помещенията с необходимото за съхранение на информацията, свързана с личните данни /папки, досиета/ обзавеждане;
- наличие на организация, гарантираща, пожаробезопасността съобразно нормативните изисквания.
2. организационни мерки:
- определяне на помещенията, в които ще се обработват лични данни, както и на тези, в които ще се разполагат елементите на комуникационно-информационните системи за обработване на лични данни, вкл. и определяне на организацията на физическия достъп
- определяне на зони с контролиран достъп;
- определяне характеристиките на физическата среда и зоните с контролиран достъп;
- определяне на помещенията, в които се разполагат елементите на комуникационно-информационните системи за обработване на лични данни;
- определяне на организация на физическия достъп;
- определяне на основни технически средства за физическа защита.
- мерки за персонална защита, представляваща система от организационни мерки спрямо физическите лица, които обработват лични данни по указание на Китка, включват:
- познаване и спазване на нормативната уредба в областта на защитата на личните данни;
- познаване на политиката и ръководствата за защита на личните данни;
- спазване на политика на чисто бюро и чист екран;
- несподеляне на критична информация между персонала (напр. идентификатори, пароли за достъп и др.);
- поверителност и задължение за неразпространение наличните данни;
- обучение на служителите, обработващи лични данни;
- обучение на персонала за реакция при събития, застрашаващи сигурността на личните данни;
- определени начини за персонална защита.
- мерки за документална защита, представляваща система от организационни мерки при обработването на лични данни на хартиен носител, включват:
- определени условията за обработване на лични данни на хартиен носител;
- регламентиран достъп на отговорните служители до регистрите, поддържани на хартиен носител;
- определен контрол на достъпа до регистрите, поддържани на хартиен носител;
- определени срокове и условия за съхранение на личните данни на хартиен носител;
- определени правила за размножаване и разпространение на хартиените носители с лични данни;
- създадени процедури за унищожаване на хартиени носители с лични данни.
- мерки за защита на автоматизирани информационни системи и/или мрежи, представляваща система от технически и организационни мерки за защита от незаконни форми на обработване на личните данни, включват:
- определени начини за идентификация и автентификация на потребителите;
- определени начини за осъществяване на телекомуникации и отдалечен достъп;

- необходими мерки за защита от вируси;
- предприети необходими мерки за поддържане/експлоатация на информационните системи и/или мрежи;
- определени начини за съхраняване на копия/резервни копия на информация с възможност за възстановяване;
- определени видове носители на информация;
- определени характеристики на физическата среда/обкръжението;
- определени начини за персонална защита;
- определени срокове за съхранение на личните данни в електронен вид;
- създадени правила за унищожаване/заличаване/изтриване на електронни носители.

Мерките са съобразени със съвременните технологични постижения и осигуряват ниво на защита, което съответства на рисковете, свързани с дейностите по обработка и категорията на защитените данни.

В допълнение Китка следва да предприеме и следните технически и организационни мерки:

- Личните данни върху технически носител се съхраняват в определени шкафове в кабинетите на съответните служители, които в извънработно време се заключват.
- Личните данни не се изнасят от сградите на кооперацията, освен при служебна необходимост и/или разрешение.
- Личните данни, организирани и съхранявани в електронен вид, се въвеждат на твърд диск на сървър от компютърната мрежа, в случай, че се обработват от повече от един служител. Компютрите, на които се обработват лични данни и се осигурява достъп до такива, са свързани в локалната мрежа със защитен достъп до личните данни, с който може да работи само обработващият лични данни. На служебните компютри се обработват лични данни, при спазване на политиките за контролиран достъп (потребителско име, парола, антивирусна защита и др.)
- При работа с личните данни се използват съответните софтуерни продукти за обработка на същите, включително относно управлението на човешките ресурси, възнагражденията на персонала, в това число основни и допълнителни възнаграждения, данъчни и други (вноски по заеми, запори и пр.) задължения, трудов стаж, присъствени и неприсъствени дни и други подобни и относно служителите на Администратора.
- Достъп до операционната система, съдържаща файловете за обработка на лични данни, имат само отговорните служители, обработващи лични данни чрез персонална парола за отваряне на тези файлове, известна само на съответния служител, а в негово отсъствие - на прекия му ръководител или друг служител, изрично определен за целта.
- Компютрите за обработка на лични данни се поставят в отделни помещения за работа, а когато не е налице организационно-техническа възможност за това, компютрите могат да бъдат поставени в общо помещение за работа.
- За повишаване сигурността на обработката на лични данни съгласно чл. 32 на Регламента, Китка може да въвежда допълнителни организационни, технологични и технически мерки, за да гарантира постоянна наличност, поверителност и цялостност на личните данни.

ЗАДЪЛЖЕНИЯ НА СЛУЖИТЕЛИТЕ НА КИТКА

Служителите на Китка обработват лични данни в съответствие с нормативната уредба в областта на защитата на личните данни и политиките, процедурите и инструкциите за защита на личните данни на кооперацията.

За неизпълнение на задълженията, вменени на съответните лица по тази политика и другите, приети политики, процедури и инструкции за защита на личните данни в Китка,

се налагат дисциплинарни наказания по Кодекса на труда, а когато неизпълнението на съответното задължение е констатирано и установено от надлежен орган – предвиденото в Закона за защита на личните данни административно наказание – глоба. Ако в резултат действията на съответното длъжностно лице по обработване на лични данни са произтекли вреди за трето лице, същото може да потърси отговорност по реда на общото гражданско законодателство или по наказателен ред, ако извършеното нарушение представлява престъпление, за което се предвижда наказателна отговорност.

ПОДДРЪЖКА И КОНТАКТ

Преразглеждането и поддържането на настоящата политика е отговорност на Правния отдел на кооперацията. Запитвания и искания във връзка с упражняването на правата на субектите на лични данни следва да бъдат насочени към kitka@kitka.bg