„ХМЦ” АД

Дружествена политика за защита на личните данни

твърдена със Заповед № ЧР 18-17-1/16.05.2018 г. на изп. директор Иво Василев

В сила от ***25 май 2018 година***

Съдържание

Въведение 4
Дефиниции 4
Декларации 6
Отговорности роли съгласно ОРЗД 7
Принципи за защита на данните 7
Права на субектите на данни 10
Съгласие 10
Сигурност на данните 10
Разкриване на данни 11
Запазване и унищожаване на данни 11
Политика за „Чисти бюра“ 12
Видеонаблюдение 12
Списък на ревизиите 13
Приложения 14
ПРИЛОЖЕНИЕ №1: ПОЛИТИКА ЗА СЪХРАНЕНИЕ НА ЛИЧНИТЕ ДАННИ 15
ПРИЛОЖЕНИЕ №2: СТАНДАРТ ЗА ОЦЕНКА НА ВЪЗДЕЙСТВИЕТО ВЪРХУ ЗАЩИТАТА НА ДАННИТЕ 6
ПРИЛОЖЕНИЕ №3: ПРОЦЕДУРА ЗА ИЗВЕСТЯВАНЕ ПРИ НАРУШЕНИЕ В СИГУРНОСТТА НА ДАННИТЕ 9
ПРИЛОЖЕНИЕ №4: ПРОЦЕДУРА ЗА РАЗГЛЕЖДАНЕ НА ЗАЯВЛЕНИЯ ЗА УПРАЖНЯВАНЕ НА ПРАВА НА СУБЕКТИТЕ НА ДАННИ 11
ПРИЛОЖЕНИЕ №5: ПРОЦЕДУРА ЗА ОБУЧЕНИЕ НА СЛУЖИТЕЛИТЕ 13

Въведение

(1) *Считано от 25 май 2018 влиза в сила Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО* ***(Общ регламент относно защитата на данните, ОРЗД)****, с който се променя съществуващият правен режим по защита на данните и свободното движение на същите.*

(2) *Като организация, установена на територията на Република България и обработваща данни на граждани на ЕС, за "ХМЦ" АД, ЕИК: 203877597, със седалище и адрес на управление в гр. Пловдив, п.к. 4004, район – Южен, бул. „Ал. Стамболийски" №9А, представлявано от изпълнителния директор Иво Кирилов Василев* ***("ХМЦ")*** *възникват редица задължения, свързани с обработването на личните данни и тяхното свободно движение в съответствие с ОРЗД, Насоките на Работната група по чл.29 от Директива 95/46/ЕО, актовете на Европейския надзорен орган по защита на данните и останалите правни актовете по защита на данните от действащото европейско и вътрешно национално законодателство („****Приложимото право"****).*

(3) *С оглед на това "ХМЦ" прие настоящата Дружествена политика за защита на личните данни* ***(„Дружествената политика")****, която, ведно с приложенията към нея, както и всякакви стандарти, оценки на въздействието и други правни актове урежда правилата за защита и обработване на личните данни и осигурява отчетността на "ХМЦ" в качеството му на администратор на лични данни:*

Дефиниции

- **"Лични данни"** означава всяка информация, свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано; физическо лице, което може да бъде идентифицирано, е лице, което може да бъде идентифицирано пряко или непряко, по-специално чрез идентификатор като име, ЕГН, постоянен или настоящ адрес, IP адрес или по един или повече признаци, специфични за физическата, физиологичната, генетичната, психическата, умствената, икономическата, културната или социална идентичност на това физическо лице.
- **"Специални категории лични данни"** означава лични данни, разкриващи расов или етнически произход, политически възгледи, религиозни или философски убеждения или членство в синдикални организации, както и обработването на генетични данни, биометрични данни за целите единствено на идентифицирането на физическо лице, данни за здравословното състояние или данни за сексуалния живот или сексуалната ориентация на физическото лице.
- "**Администратор"** по смисъл на настоящата Дружествена политика означава "ХМЦ" АД, в случаите когато определя целите и средствата за обработването.

- **“Обработващ”** означава всяко лице, различно от “ХМЦ” и служителите му, което обработва Личните данни от името на “ХМЦ”. Обработващи са съконтрахентите, на които “ХМЦ” е възложило дейност по обработване и с които в качеството си на Администратор сключва договори или други правни актове по смисъла на чл.28, пар.3 от ОРЗД, уреждащи защитата и обработването на Личните данни.

- **“Субект на данни”** означава всяко физическо лице, за което Личните данни се отнасят. По смисъла на Дружествената политика субекти на данни са бившите и настоящи служители на “ХМЦ”, кандидатите за работа, клиентите на “ХМЦ”, както и служителите и клиентите на контрахентите на “ХМЦ”, в случаите, в които последното обработва техни лични данни.

- **“Обработване”** означава всяка операция или съвкупност от операции, извършвана с Личните 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.

- **“Профилиране”** означава всяка форма на автоматизирано обработване на лични данни, предназначена за оценяване на определени лични аспекти, свързани с физическо лице, или за анализиране или прогнозиране на изпълнението на професионалните задължения на това физическо лице, неговото икономическо състояние, местоположение, здраве, лични предпочитания, надеждност или поведение. Доколкото “ХМЦ” не извършва дейност по профилиране ще предостави информация на субектите на данни, че правото да се противопоставят на профилирането, на мерките, основаващи се на профилирането и на предвидените последици от профилирането върху лицето са неприложими.

- **"Нарушение на сигурността на лични данни”** означава 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. “ХМЦ” има задължението да уведоми Надзорния орган за нарушения и/или да съобщи на Субектите на данни тогава, когато има вероятност нарушението да има неблагоприятни последици върху данните или неприкосновеността на личния им живот.

- **“Заявление за упражняване на права на Субектите на данни съгласно ОРЗД”** или **“Заявление съгласно ОРЗД”** означава всяко искане, отправено на посочените от "ХМЦ” данни за контакт, засягащо упражняване на едно или няколко права, предвидени в Глава трета от ОРЗД. "ХМЦ” ще разгледа в срок от един месец и безплатно всяко такова зявление, стига последното да не е ексесивно, да не позволява ясно идентификацията на Субекта на данни или да не налага прекомерни разходи за Администратора.

- **“Съгласие на субекта на данните”** - означава всяко свободно изразено, конкретно, информирано и недвусмислено указание за волята на Субектите на данните, посредством изявление или ясно потвърждаващо действие, което изразява съгласието му личните му данни да бъдат обработени. “ХМЦ” събира използва съгласие на Субектите като основание за обработване само за целите на осъществяването на маркетинг или когато не може да бъде изтъкнато друго легитимно законово основание.

- **“Дете”** означава всяко лице на възраст под 16 години или по-ниска възраст, в случай, че такава бъде определена в националното законодателство по защита на данните. Обработването на лични данни на дете е законосъобразно само ако е получено съгласие на родител или настойник.
- **“Трета страна”** означава физическо или юридическо лице, публичен орган, агенция или друг орган, различен от субекта на данните и администратора.
- **“Надзорен орган”** означава Комисията за защита на личните данни (КЗЛД) или друг компетентен орган по защита на данните, определен в съответствие с Приложимото право.
- “**Регистър с лични данни”** означава всеки структуриран набор от лични данни, достъпът до които се осъществява съгласно определени критерии, независимо дали е централизиран, децентрализиран или разпределен съгласно функционален или географски принцип**.**

Декларации

(1) “ХМЦ” се ангажира да спазва всички правни актове на ЕС и на Република България относно защитата на личните данни, както и да защитава и способства упражняването на правата на субектите, чиито данни събира и обработва.

(2) Настоящаща Дружествена политика, ведно със свързаните с нея процедури и стандарти, цели осигуряване на механизми за правно съответствие и гарантиране на спазването на ОРЗД.

(3) Приложимото право и Дружествената политика, ведно с приложенията към нея, се прилагат за всички дейности, свързани с обработване на лични данни, които “ХМЦ” обработва.

(4) В съответствие със Стандарта за извършване на оценка на въздействието върху защитата на данните посоченото/ите във Дружествената политика лица за защита на данните отговарят за преглеждането на всеки нов процес, който предстои да бъде имплементиран и който касае обработването на лични данни, както и за преглеждане на настоящата политика и приложенията към нея, както и на всички дейности по обработване **поне веднъж на всеки две години** с оглед на всякакви промени в осъществяваните процеси, свързани с обработване на Личните данни (т.нар. *принцип за защита на данните на етапа по проектиране и по подразбиране*).

(5) Дружествената политика се прилага за всички служители и представители на “ХМЦ”, както и за техните съконтрахенти и други обработващи Личните данни, като например системни администратори и фирми за IT поддръжка, собственици на външни сървъри, доставчици, туроператори и дружества за изнесено счетоводство. Всяко нарушение на Приложимото право или на Дружествената политикаще бъде разглеждано съгласно дисциплинарната политика на Администратора и може да бъде престъпление, като в този

случай въпросът ще бъде докладван във възможно най-кратък срок на съответните органи.

(6) Контрахентите и всички трети страни, които работят с или за Администратора, и които имат или могат да имат достъп до Личните данни, трябва да са прочели, разбрали и да са се задължили да спазват настоящата Дружествена политика.

(7) Трети страни не може да имат достъп до Личните данни без предварително да са сключили споразумение за поверителност на данните, което им налага задължения не по-малко обременяващи, от тези, с които се е ангажирала "ХМЦ" в настоящата Дружествена политика и което Администраторът има право да проверява.

Отговорности роли съгласно ОРЗД

1. "ХМЦ" е администратор и/или обработващ лични данни съгласно ОРЗД.
2. Всички лица, които изпълняват управленски или надзорни роли в "ХМЦ", са отговорни за разработването и насърчаването на добри практики за обработване, като отговорностите са посочени в индивидуалните длъжностни характеристики.
3. Спазването на законодателството за защита на данните е отговорност на всички служители и представляващи "ХМЦ", които обработват лични данни.
4. Процедурата за обучение на служителите определя конкретните изисквания за обучение и осведоменост във връзка с ролите и отговорностите на служителите съгласно ОРЗД като цяло.
5. Служителите са отговорни да гарантират, че всички лични данни, свързани с тях и предоставени от тях на съответната организация, са точни и актуални.

Принципи за защита на данните

Всяко обработване на лични данни трябва да бъде извършвано в съответствие с принципите за защита на данните съгласно разпоредбите на член 5 от ОРЗД. Дружествената политика гарантира спазването на тези принципи.

<u>Личните данни трябва да бъдат обработвани законосъобразно, добросъвестно и прозрачно</u>

- *Законосъобразно* - определете правно основание, преди да обработвате личните данни. Често тези условия са наричани "условия за обработване", например съгласие.
- *Добросъвестно* - "ХМЦ" прави определена информация достъпна за Субектите на данни, доколкото е практически приложимо. Това се прилага, независимо дали Личните данни са получени пряко от Субекта на данните или от други източници.
- *Прозрачно* - ОРЗД има повишени изисквания относно това каква информация трябва да бъде достъпна за Субектите на данни, което е в обхвата на изискването за "прозрачност". Изискването за прозрачност включва правила относно предоставяне на Субектите на данните на информацията по членове

12-14 под формата на **известие за поверителност/уведомление за обработване на лични данни**. Те се изготвят в разбираема и достъпна форма, на ясен и прост език, и включва най-малко:

- данните, които идентифицират "ХМЦ", включително данни за контакт, както и за нейните представители;
- координатите за връзка с длъжностното лице за защита на данните, в случай, че такова бъде назначено;
- целите на обработването, за което Личните данни са предназначени, както и правното основание за обработването;
- срокът, за който се съхраняват Личните данни;
- съществуването на правата да се изиска достъп, коригиране, изтриване или възражение срещу обработването, както и условията, свързани с упражняване на тези права;
- съответните категории обработвани лични данни;
- получателите или категориите получатели на личните данни;
- когато е приложимо, намерението на администратора да предаде личните данни на трета държава и нивото на защита, осигурявано за данните;
- всякаква необходима допълнителна информация за да се гарантира добросъвестно обработване.

Личните данни могат да бъдат събирани единствено за конкретни, изрично указани и легитимни цели.

Личните данни трябва да бъдат подходящи, свързани с и ограничени до необходимото за обработването.

Личните данни трябва да бъдат точни и да се поддържат актуални, като се полагат всички усилия за своевременното изтриване или коригиране

- Данните, които се съхраняват от "ХМЦ", трябва да бъдат преглеждани и актуализирани, когато е необходимо. Не се съхраняват данни, ако не може основателно да се приеме, че са точни.
- **Всички формуляри, чрез които се събират лични данни, включват декларация на субектите, че предоставените данни са точни и актуални.** При съществени промени в данните с оглед поддържане на тяхната точност и актуалност, субектите на данни ще уведомят Администратора.

Личните данни трябва да бъдат съхранявани във форма, която да позволява идентифицирането на субекта на данните за период, не по- дълъг от необходимото за обработването:

- Когато личните данни са запазени след датата на обработване, те ще бъдат анонимизирани, псевдономизирани и/или сведени до минимум с цел да се запази самоличността на субекта на данните в случай на нарушение на сигурността на данните.
- Личните данни се съхраняват в съответствие с посочените по-долу срокове за съхранение, след изтичането на които данните ще бъдат унищожени по сигурен начин.

Личните данни трябва да бъдат обработвани по начин, който гарантира подходящо ниво на сигурност.

При определяне на подходящото ниво на сигурност “ХМЦ” взема под внимание степента на евентуалните вреди или загуби, които могат да бъдат причинени на лицата, ако възникне нарушение в сигурността на данните, последиците от нарушението и възможното накърняване на репутацията.

При оценяване на подходящите организационни мерки “ХМЦ” има предвид следното:

- подходящите нива на обучение в организацията;
- мерки, които отчитат надеждността на служителите;
- включване на разпоредби относно защитата на данните в трудовите и/ или гражданските договори;
- определяне на дисциплинарни мерки при нарушение на правилата по защита на данните;
- наблюдение на персонала за спазване на съответните правила за защита на данните;
- проверки на физическия достъп до лични данни в електронен вид и на хартиен носител;
- приемане на политика за “чисти бюра”;
- съхраняване на данни на хартиен носител в заключващи се огнеупорни шкафове;
- ограничаване използването на преносими електронни устройства извън работното място;
- ограничаване използването на лични устройства на служителите, които се използват на работното място;
- приемане на ясни правила за паролите, позволяващи индивидуална идентификация на всеки служител на Администратора, разполагащ с достъп до Личните данни на база “Необходимост да знае”;
- осъществяване на охранителна дейност, регистриран режим на достъп посредством чип-карти на служителите и извършване на видеонаблюдение в помещенията на “ХМЦ”.
- редовно създаване поне два пъти месечно на резервни копия от Личните данни на електронни сървъри, локализирани в ЕИП;

<u>Администраторът на данни трябва да е в състояние да докаже спазването на останалите принципи на ОРЗД (“отчетност”)</u>

ОРЗД включва разпоредби, които насърчават отчетността като допълнение на изискванията за прозрачност. “ХМЦ” доказва спазването на принципите за защита на личните данни като прилага настоящата Дружествена политика и приложенията към нея, спазва етични кодекси за поведение, прилага технически и организационни мерки за защита на данните, както и като прилага принципа на защита на данните в етапа на проектиране и по подразбиране, както и като изготвя оценки на въздействието при дейности по обработване, свързани с висок

риск за правата и свободите на субектите на данни в съответствие със Стандарта за оценката на въздействие върху защитата на данните.

Права на субектите на данни

1. Субектите на данни имат следните права относно обработването на данни и данните, които са записани за тях:
   1.1. да подават искания за достъп на субекта по отношение на естеството на съхраняваната информация и на кого е била разкрита;
   1.2. да предотвратяват обработване, което може да предизвика вреди или страдание;
   1.3. да предотвратяват обработване за целите на директния маркетинг;
   1.4. да завеждат дела за обезщетение на действително претърпените вреди поради нарушение на ОРЗД от страна на "ХМЦ";
   1.5. да предприемат действия за коригиране, блокиране, изтриване, включително правото "да бъдат забравени", или за унищожаване на неточни данни;
   1.6. да поискат от Надзорния орган да оцени дали разпоредба на ОРЗД е била нарушена;
   1.7. личните данни да им бъдат предоставени в структуриран, широкоизползван и пригоден за машинно четене формат и правото тези данни да бъдат прехвърлени на друг администратор;
2. "ХМЦ" способства упражняването на правата на субектите на данните по реда, предвиден в Процедурата за разглеждане на заявления за упражняване на права на субектите на данни съгласно ОРЗД.

Съгласие

1. "ХМЦ" разбира, че "съгласие" означава **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. Съгласието може да бъде оттеглено по всяко време.
2. "ХМЦ" разбира, че "съгласие" означава, че субектът на данните е напълно информиран за планираното обработване и е изразил съгласието си в здравословно психическо състояние и без да му е упражняван натиск. Съгласие, получено по принуда или въз основа на подвеждаща информация, няма да бъде валидно основание за обработване.
3. Трябва да има активна комуникация между страните с цел доказване на активно съгласие. Не може да бъде заключено, че има съгласие при липса на отговор на съобщение или противопоставяне на общи условия на дадена организация.

Сигурност на данните

1. Всички служители носят отговорност да осигурят необходимите условия личните данни, обработвани в рамките на процесите, осъществявани в съответната организация и за които те носят отговорност, да се съхраняват по сигурен начин и да не се оповестяват на трета страна при никакви

условия, освен ако тази трета страна не е специално упълномощена от организацията да получава тази информация и не е сключила споразумение за поверителност.

2. Всички лични данни трябва да бъдат достъпни само за лицата, които се нуждаят от тях на принципа “Необходимост да знае”. Всички лични данни трябва да бъдат разглеждани с най-висока степен на сигурност и трябва да бъдат съхранявани:
   - в стая с контролиран достъп, която се заключва, и/или
   - в заключено чекмедже или шкаф, и/или
   - ако са в електронен формат, със защитена парола съгласно фирмените изисквания и/или
   - на (преносими) електронни носители, които са криптирани.

3. Трябва да се положат грижи за гарантиране, че екраните на компютрите и терминалите не се виждат от други лица, освен от упълномощените служители на организацията.

4. Ръчните записи не могат да бъдат оставени на места, където могат да бъдат достъпни за неоторизирани лица.

5. Личните данни могат да бъдат изтрити или унищожени в съответствие с Политиката за съхранение на данни.

Разкриване на данни

1. “ХМЦ” гарантира, че личните данни няма да бъдат разкривани на неупълномощени лица - членове от семейството, приятели, правителствени органи и в определени обстоятелства - полицията. Всички служители трябва да бъдат внимателни, когато бъдат помолени да разкрият на трета страна лични данни, съхранявани за друго лице и ще бъдат длъжни да присъстват на специално обучение, което ще им позволи да се справят ефективно с такъв риск. Важно е да се има предвид дали разкриването на информацията е свързано с и необходимо за извършване на дейността на организацията.

2. Всички искания за предоставяне на данни по една от тези причини трябва да бъдат съпроводени от подходящи документи и **за всички оповестявания трябва да има специални разрешения от страна на определеното лице за защита на данните**.

Запазване и унищожаване на данни

1. “ХМЦ” не съхраняват лични данни във форма, която да позволява идентифицирането на субекта на данните за период, не по-дълъг от необходимото във връзка с целите, за които данните са първоначално събрани.
2. “ХМЦ” може да продължи да съхранява лични данни ако последните биват обработвани единствено за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели, при

условие че бъдат приложени подходящите технически и организационни мерки с цел да бъдат гарантирани правата и свободите на субекта на данните.

3. Срокът на запазване за всяка категория лични данни е посочен в Политиката за съхранение на данни.
4. Личните данни трябва да бъдат унищожени по сигурен начин в съответствие с ОРЗД - данни са обработвани по подходящ начин с цел поддържане на сигурността, като по този начин се защитават правата и свободите на субектите на данните. Всяко унищожаване на данни се извършва в съответствие с Политиката за съхранение на данните.

Политика за „Чисти бюра“

Не оставяйте документи върху бюрата си или по отворени рафтове в близост до тях, когато не сте на работното си място за по-дълго време (над 20 мин.). Секретни и документи с чувствителен характер не се оставят без надзор при никакви условия. Всички служители на „ХМЦ“ отговарят за сигурността и безопасността на информацията, била тя на хартиен или електронен носител, и поверените им активи.

Заключвайте кабинетите си и почиствайте бюрата преди да напуснете сградата. В края на работния ден вие сте длъжни да почистите бюрата си, да изключите осветлението и климатиците, и да заключите вратите на кабинетите. Всички чекмеджета и шкафове трябва да са заключени докато служителят, на когото са дадени, е извън сградата и в неработно време. Всички шкафове в общите помещения имат собственик, който е задължен да пази ключовете и да държи шкафа си заключен в извънработно време.

Служителите се задължават винаги да носят със себе си ключовете от кабинетите, чекмеджетата, шкафовете и други поверени им контейнери, в които се съхраняват документи, или да ги държат под ключ. Ключовете, раздавани на доверени офис асистенти (определени със заповед на мениджър „Човешки ресурси” – обикновено офис асистенти на висшето ръководство) се третират по същия начин. Всяка ключалка има пореден номер, който е изписан на ключа, който я отваря. Копия от ключовете се съхраняват от мениджъра по сигурността, или упълномощено от него лице, в сейф. Сейфът с ключовете се монтира върху стена или се съхранява в друг, по-голям сейф. Мениджърът по сигурността, или упълномощено от него лице, води регистър за всички ключове в обръщение, и издава копия, ако са необходими докато притежателят на оригиналите не е на разположение.

Видеонаблюдение

В случаите, когато “ХМЦ” осъществява видеонаблюдение като дейност, свързана с обработването на лични данни, ще съхранява данните за **минимален срок от един месец**, определен в Политиката за съхранение на данните. Видеонаблюдението се извършва само на изрично означените с уведомление за видеонаблюдение и/или стикери за видеонаблюдение, реферирaщи към уведовлението места на база легитимния интерес на “ХМЦ” да осигури сигурността на служителите и имуществото си, без по никакъв начин да засяга правата и достойнството на субектите на данни (така например организациите няма да осъществяват видеонаблюдение в тоалетни помещения, зали за почивка и така нататък).

Списък на ревизиите

Версия 1, 25 май 2018 година	*Изготвена и приета съгласно Общия регламент относно защитата на данните*
Версия 2,24.07.2018 г.	

Приложения

Приложение №1	**Политика за съхранение на личните данни**
Приложение №2	**Стандарт за извършване на оценка на въздействието на риска върху защитата на данните**
Приложение №3	**Процедура за известяване при нарушение на сигурността на личните данни**
Приложение №4	**Процедура за разглеждане на заявления за упражняване на права на субектите на данни съгласно ОРЗД**
Приложение №5	**Процедура за обучение на служителите**

ПРИЛОЖЕНИЕ №1:
ПОЛИТИКА ЗА СЪХРАНЕНИЕ НА ЛИЧНИТЕ ДАННИ

Обхват
Всички лични данни, обработвани от "ХМЦ", са обект на изискванията за съхраняване и унищожаване на лични данни, предвидени в настоящата политика.

Отговорности
1. *Собствениците на лични данни* носят отговорност за събирането, съхраняването и унищожаването на личните данни в съответствие с изискванията на ОРЗД.

2. *Собственик на данните* е ръководителят на съответния отдел в рамките „ХМЦ", в който се осъществява процесът по обработване на личните данни. Собствениците на информация са:

Изп.директор	Иво Василев
Специалист „Човешки ресурси"	Донна Йовчева
Директор Предприятие	Росен Стоилов
Главен счетоводител	Светлана Гочева
Отговорник по правните въпроси/юрисконсулт/	Иванка Шикова
Отговорник по охраната и сигурността	Владимир Шекеримов

3. Главният счетоводител отговаря за събирането, съхранението и унищожаването на финансовите (счетоводни, данъчни) и свързаните с тях записи.
4. Специалист "Човешки ресурси" отговаря за събирането, съхраняването и унищожаването на всички документи и архиви с документи, свързани със служителите на "ХМЦ", полагащи труд по трудов или граждански договор (**човешките ресурси**).
5. Директор предприятие отговаря за събирането, съхраняването и унищожаването на всички документи, съдържащи лични данни и свързани с търговските отношения с контрагентите на „ХМЦ".
6. Отговорникът за охраната и сигурността отговаря за видеозаписите и регистрите за достъп до помещенията на "ХМЦ".
7. Изпълнителният директор осъществява общ надзор върху спазването и изпълнението на ОРЗД и при необходимост реферира останалите собственици на данни към Отговорника по правни въпроси.
8. Отговорникът по правни въпроси отговаря за събирането, съхраняването и унищожаването на всички документи, свързани с упражняването и защитата по правни претенции, както и консултира изпълнителния

директор при осъществяването на общ надзор по отношение на изпълнението на ОРЗД.

Срокове за съхранение на лични данни

Необходимите срокове на съхранение на отделните категорията лични данни се определят както следва:

Субекти на данни	Срок за съхранение	Начален момент, от който тече срокът	Правно основание	Видове документи	Собственик на данните
Човешки ресурси	5 години	Началото на финансовата година, през която са съставени	Изпълнение на трудовия или граждански договор.	Всички данни и записи на данни от трудовото досие на служителя, за които не е приложим законово определен срок (например за ведомости)	Директор ЧР
Кандидати за работа	1 година	Датата на приключване на кампанията по набиране на персонал		Всички документи, предоставени на Дружеството по повод провеждането на кампанията по набиране на персонал	Директор ЧР
Бивши служители/ Служители	50 години	Месец януари на отчетния период, следващ счетоводния период, за който документите се отнасят	Чл. 12 от ЗСч, чл. 38 от ДОПК	Данни за заплати, данни от ведомости	Директор ЧР

Клиенти на услуги / доставчици	10 години	Месец януари на отчетния период, следващ счетоводния период, за който документите се отнасят	Чл. 12 от ЗСч, чл. 38 от ДОПК	Счетоводни записи и финансови извлечения, включително документи за данъчен контрол, одити и последващи финансови инспекции	Финансов директор
Лице, което може да заведе иск срещу организацията	5 години		Чл. 110-111 от ЗЗД	Всички документи могат да се съхраняват от Дружеството с оглед осъществяване на защитата му срещу потенциалния иск	Отговорник по правни въпроси
Лица, ангажирани с маркетинг дейности	1 година, освен ако е основано на съгласие и то не бъде подновено	Краят на маркетинг кампанията		Бизнес комуникация с клиенти/ документи, отнасящи се популярността на марката	Директор Маркетинг
Служители	30 дни	Датата на видео записа	Легитимен интерес	Записи от видеонаблюдение	Отговорник по охраната и сигурността

Доставчици/ контрагенти/ лица, имащи връзка със сделки "ХМЦ"	5 години	Началото на годината след сключването на сделката или прекратяване на правоотношението	Чл. 67, ал. 1 от ЗМИП	Всякакви документи и информация във връзка със задълженията, произтичащи от ЗМИП	Търговски директор

Субекти на данни	Срок за съхранение	Начален момент, от който тече срокът	Правно основание	Видове документи	Собственик на данните
Субекти подали заявление съгласно ОРЗД	3 години	Получаване на заявление		Искания от Субекти на данни; Жалби от Субекти на данни	Отговорник по правни въпроси
Субекти - подали заявления съгласно ОРЗД	3 години	Изпращане на отговор до Субект на данни		1. Отговори на искания от Субекти на данни 2. Отговори на жалби от Субекти на данни	Отговорник по правни въпроси
Клиенти на ХМЦ	3 години	Датата на последната обработка на данни, основана на Известието		Известия за поверителност за клиенти на "ХМЦ"	Отговорник по правни въпроси

Клиенти и потенциални клиенти	3 години	Дата на последната обработка на данни, основана на съгласие		Форми за съгласие	Отговорник по правни въпроси
Всички субекти на данни	3 години	Датата на инцидента или датата, на която е узнато за инцидента		Документи, свързани с нарушения на сигурността на личните данни Уведомления относно нарушенията	Отговорник по правни въпроси
Субекти, чиито лични данни фигурират във вътрешните документи на ХМЦ	3 години	Датата, от която документите вече не са в сила		Политики, процедури и други вътрешни документи, отнасящи се до лични данни	Отговорник по правни въпроси

Унищожаване на лични данни

Всеки собственик на данни отговаря за унищожаването на подведомствените му данните след изтичане на срока за тяхното съхранение. Унищожаването трябва да се извърши до 30 дни клед изтичнето на срока за съхранение по следния ред:

(1) Собственикът на данните констатира, че срокът за съхранение на даден документ или архив с документи е изтекъл, и уведомява отговорника по правните въпроси.

(2) Отговорникът по правни въпроси проверява дали не е налице основания за продължаване на съхранението на документа, въпреки изтичането на срока. Ако такова е налице Отговорникът по правните въпроси отбелязва правното основание и допълнителният срок за съхранение.

(3) Ако правно основание не е налице Собственикът на данните унищожава документа или архивът с документи, съдържащи лични данни, като съставя протокол за унищожение на данните. Отговорникът по правни въпроси приподписва всеки протокол за унищожение, с което потвърждава липсата на правно основание продължаване на съхранението.

(4) Унищожаването се извършва, както следва: чрез **шредиране** на документите, съдържащи личните данни, срокът за чието съхранение е изтекъл, или чрез **изтриване/заличаване** на електронни документи и всички техни резерзви копия.

(5) В случай, че унищожаването на документите се прави по повод заявление от субект на данните съгласно ОРЗД, след унищожаване на данните Отговорникът по правните въпроси уведомява Изпълнителния директор за всички получатели на данните, ако са налице такива. В съответствие с ОРЗД Изпълнителният директор гарантира унищожаването на всички копия от данните като отправя предизвестие до получателите на данните за тяхното унищожаване.

ПРИЛОЖЕНИЕ №2: СТАНДАРТ ЗА ОЦЕНКА НА ВЪЗДЕЙСТВИЕТО ВЪРХУ ЗАЩИТАТА НА ДАННИТЕ

Обхват

Всички проекти, които включват обработване на лични данни или всички действия (както вътрешни, така и външни), които засягат обработването на лични данни и оказват въздействие върху неприкосновеността на личния живот на субектите на данните, попадат в обхвата на настоящия стандарт и ще бъдат обект на оценка на въздействието върху защитата на данните.

Отговорности

1. Отговорникът по правни въпроси отговаря за извършването на периодични и предварителни проверки относно защитата на личните данни с цел установяване на необходимостта от извършване на оценка на въздействието върху защитата на данните.

2. Периодичните проверки включват преглед на всички процеси във “ХМЦ”. Периодичните проверки се провеждат поне веднъж на всеки две години.

3. В изпълнение на принципа за защита на данните на етапа по проектиране и по подразбиране се провеждат предварителни проверки за необходимост от извършване на оценка на въздействието върху защитата на данните преди имплементирането на всеки процес в “ХМЦ”. Всеки собственик на данните носи отговорност да уведоми Отговорника по правните въпроси за имплементирането на процесите в неговия отдел, които са свързани с лични данни.

4. Когато по време на периодична или предварителна проверка Отговорникът по правни въпроси констатира, че е налице необходимост от извършване на оценка на въздействието върху защитата на данните, той уведомява изпълнителния директор и извършва оценката по методологията, посочена по-долу.

5. Собствениците на данни - ръководителни на отделите, обработващи личните данни, за които е идентифициран риск, са отговорни за прилагането на всякакви идентифицирани решения за риска от нарушение на неприкосновеността на личния живот.

Процедура

В случай, че Отговорникът по правни въпроси определи необходимост от извършване на оценка на въздействието върху защитата на данните при периодична или предварителна проверка, като оценява проекта и вида лични данни, свързани с него или дейността по обработване, използва долупосочените критерии и следва матрицата на вероятностите и въздействието.

Матрица на вероятностите:

Вероятност	0	3	6	9
	0	2	4	6
	0	1	2	3
	0	1	2	3
	Въздействие			

Рискове за правата и свободите на субектите на данните:

Ниво на риска	От	До	Оценка съгласно ОРЗД
Високо	6	9	Най-висок неприемлив риск
Средно	3	5	Неприемлив риск
Ниско	1	2	Приемлив риск
Нулево	0	0	Няма риск

Идентифициране на рискове за неприкосновеността на личния живот

1. Отговорникът по правните въпроси оценява рисковете за неприкосновеността на личния живот на субектите на данни за всяка дейност по обработка, както е описано по-горе, като:

   - определя и описва риска за неприкосновеността на личния живот, свързан с тази дейност от процеса;

- използва критериите за вероятност (1 - ниско, 2 - средно и 3 - високо) и оценява вероятността за възникване на риск
- използва критериите за въздействие (0 - нулево въздействие, 1 - ниско, 2 - средно и 3 - високо) на риска, ако той възникне;
- пресметне риска чрез идентифициране на риска за правата и свободите на субектите на данните.

2. При оценяване на рисковете за неприкосновеността на личния живот Отговорникът по правните въпроси взема под внимание рисковете за правата и свободите на физическите лица, произтичащи от обработването на лични данни; рисковете за бизнеса (включително накърняване на репутацията) и целите и задълженията за обработване (както по закон, така и въз основа на договор).

3. Отговорникът по правните въпроси идентифицира решения за рисковете за неприкосновеността на личния живот и заедно с Изпълнителният директор определя собственика на данни отговорен запреодоляване на риска, както и краен срок за изпълнение на предвидените мерки.

4. Отговорникът по правни въпроси заедно с Изпълнителния директор определя като приоритетни анализирани рискове въз основа на критериите за високо ниво на риска, посочени по-горе.

Предварителна консултация (член 36 от ОРЗД)

1. Когато оценката на въздействието върху защитата на данните покаже, че обработването на лични данни ще породи висок риск за субекта на данните, ”ХМЦ” може да се консултира с Надзорния орган. Това консултиране се извършва в писмена, включително електронна форма.

2. Когато “ХМЦ” поиска консултация от Надзорния орган, предоставя следната информация:
   - информация за отговорностите на организацията и лицата, които се занимават с обработването;
   - целите на планираното обработване;
   - информация за всякакви/всички мерки и контроли, които се прилагат/ предоставят за защита на правата и свободите на субектите на данни;
   - копие от оценката на въздействието върху защитата на данните и всякаква друга информация, поискана от надзорния орган.

ПРИЛОЖЕНИЕ №3:
ПРОЦЕДУРА ЗА ИЗВЕСТЯВАНЕ ПРИ НАРУШЕНИЕ В СИГУРНОСТТА НА ДАННИТЕ

Обхват

Настоящата процедура се прилага в случай на нарушение на сигурността на личните данни съгласно член 33 и член 34 от ОРЗД. Всички служители на „ХМЦ“ са длъжни да се запознаят и да спазват настоящата процедура. Всички служители, изпълнители или временно нает персонал са отговорни за докладване на нарушенията на сигурността на личните данни на Отговорника по правните въпроси и/или Изпълнителния директор.

Уведомление за нарушение от обработващ данни до администратор на данни

В случаите когато е обработващ или съвместен администратор “ХМЦ” докладва всяко подлежащо на докладване нарушение на сигурността на личните данни или инцидент, свързан със сигурността, на друг администратор личните данни без ненужно забавяне и при всички случай в срок до 72 часа от узнаване на нарушението. Информацията за нарушението се вписва в Регистъра на нарушенията на сигурността на данните („Регистъра“), като „ХМЦ“ предоставя на администратора цялата необходима информация за нарушението. Уведомяването за нарушението се извършва по имейл, факс, поща и др. данни за контакт, посочени в договора с администратора. Уведомяването се извършва от Отговорника по правните въпроси в писмена форма и получаването му се потвърждава от администратора в същата форма.

Уведомление за нарушение до надзорен орган

Изпълнителният директор след консултиране с Отговорника по правните въпроси определя дали Надзорният орган трябва да бъде уведомен в случай на нарушение на сигурността на личните данни. Преценката дали да бъде уведомен надзорния орган се извършва според това дали има вероятност нарушението да породи риск за правата и свободите на субектите на данните, въз основа на оценката за въздействието върху защитата на данните, извършена от Отговорника по правните въпроси. Ако съществува риск за субектите на данни по предложение на Отговорника по правните въпроси Отговорникът по правните въпроси докладва нарушението на Надзорния орган по-късно от 72 часа от узнаването на нарушението. Ако уведомяването не бъде извършено в рамките на 72 часа Отговорникът по правните въпроси го предава по електронен път с обосновка за забавянето. Ако не е възможно да се предостави цялата необходима информация наведнъж, Отговорникът по правните въпроси предоставя информацията на етапи без ненужно допълнително забавяне.

Уведомление за нарушение до субектите на данни

Изпълнителният директор след консултиране с Отговорника по правни въпроси определя дали субектите на данни трябва да бъде уведомени в случай на нарушение на сигурността на личните данни. Ако има вероятност нарушението на сигурността на личните данни да породи висок риск за правата и свободите на субектите на данните, Отговорникът по правните въпроси уведомява засегнатите субекти на данни в писмена, включително електронна форма, незабавно и на ясен и прост език и при всички

случай не по-късно от 72 часа от узнаване на нарушението. „ХМЦ“ впоследствие взема мерки, които гарантират, че вече няма вероятност да настъпят рискове за правата и свободите на субектите на данни.

Ако нарушението засяга голям брой субекти и техните лични данни, Изпълнителният директор след консултиране с Отговорника по правните въпроси взема решение за отправяне на публично съобщение или друга подобна мярка, въз основа на оценка на количеството усилия, необходими за уведомяването на всеки субект на данни поотделно и дали това би възпрепятствало възможността за предоставяне на уведомлението, така че засегнатите лица да бъдат в еднаква степен ефективно информирани.

Ако „ХМЦ“ не е уведомила субектите на данните и надзорният орган отчете вероятност нарушението на сигурността на личните данни да породи висок риск, Отговорникът по правните въпроси ще съобщи за нарушението по гореописания ред.

Регистър на нарушенията в сигурността на личните данни

Отговорникът по правните въпроси документира всяко нарушение в сигурността на личните данни. Нарушенията се документират като бъдат вписани в Регистъра на нарушенията в сигурността на личните данни, воден във всяка организация.

Регистърът по-специално включва следната информация:

a. категориите засегнати лични данни;
b. приблизителният брой на засегнатите субекти на данни;
c. приблизителното количество на засегнатите лични данни.
d. името и координатите за връзка на Отговорникът по правни въпроси;
e. последиците от нарушението;
f. всички предприети мерки за справяне с нарушението;
g. всякаква информация, свързана с нарушението;
h. в случай че Надзорният орган определи конкретен контакт във връзка с нарушение, тази информация също ще бъде отразена в Регистъра.

ПРИЛОЖЕНИЕ №4:
ПРОЦЕДУРА ЗА РАЗГЛЕЖДАНЕ НА ЗАЯВЛЕНИЯ ЗА УПРАЖНЯВАНЕ НА ПРАВА НА СУБЕКТИТЕ НА ДАННИ

Обхват

1. Настоящата процедура обхваща упражняването на права съгласно Глава III от ОРЗД, от субектите във връзка с обработването на личните им данни от страна на "ХМЦ", обжалването на действията на администратора от субектите на данни и относно начина, по който жалбите се разглеждат.

2. Всички служители носят отговорност да гарантират, че подадените заявления за упражняване на права и/или жалби от субекти на данни са докладвани на Отговорника по правни въпроси, който отговаря за обработването на заявленията и жалбите в съответствие с ОРЗД, Дружествената политика и настоящата процедура.

Процедура

"ХМЦ" предоставя ясни насоки на страницата си, включително под формата на извадка от Дружествената политика, както и към известието за поверителност, съдържащо информация как субектът на данните може да подаде заявление/жалба относно:

- начина, по който са били обработени личните им данни;
- начина, по който е било обработено искането за достъп до данни;
- начина, по който е била обработена жалбата им;
- да обжалват решение, взето вследствие на жалба.

Субектите на данните, подават жалба чрез имейл в свободна форма или като използват предоставени от „ХМЦ" форми, като се позоват изрично на правото си по ОРЗД и предоставят достатъчна информация за да удостоверят идентичността си, или като използват формуляра за контакт, публикуван на уебсайта на "ХМЦ". Всички жалби, включително жалбите, получени чрез формуляра за контакт, се насочват към Отговорника по правни въпроси за разрешаване.

Жалбите трябва да се разрешават в рамките на едномесечен срок, освен ако не са свързани с особенна трудност, в който случай срокът може да бъде удължен с още два месеца, след като субектът на данните бъде информира за забавянето в едномесечния срок. Подадените жалби се разглеждат в същия срок.

Ако организацията не предприеме действия по заявление на субект на данни в рамките на срока или откаже искането, длъжностното лице по защитата на данните определя на ясен и прост език причините, поради които не е предприето действие.

При всякаква комуникация със субекта на данните организацията представлявана от лицето по защитата на данните, информира субекта за правото му да подаде жалба директно до Надзорния

орган като предостави данните за контакт на надзорния орган и го информира за правото му да потърси защита по съдебен ред.

ПРИЛОЖЕНИЕ №5: ПРОЦЕДУРА ЗА ОБУЧЕНИЕ НА СЛУЖИТЕЛИТЕ

Обхват

Тази процедура се прилага за програмата за обучение и повишаване на осведомеността на служителите на "ХМЦ" по отношение на обработването на лични данни, когато същото се отнася до ОРЗД, спазването му и други въпроси, свързани със защитата на личните данни, тяхното свободно движение и неприкосновеността на личния живот.

Политика на обучение

1. Отговорникът по правните въпроси възлага отговорности по защита на данните на служителите на "ХМЦ".
2. Изпълнителният директор осигурява провеждане на обучение по защита на данните за всички служители, които имат отговорности, включващи обработване на лични данни.
3. Изпълнителният директор насърчава програмите за обучение и повишаване на осведомеността, на служителите, имащи функции по обработване на лични данни.
4. Изпълнителният директор и Отговорникът по правни въпроси гарантират, че всички изисквания за сигурност, свързани със защитата на данните, са показани и съобщени на служителите, имащи функции за защита на данните.
5. Служителите получават специално обучение за обработване на личните данни, свързани с техните индивидуални роли и отговорности, и в съответствие с политиките, стандартите и процедурите на "ХМЦ".
6. Служителите получават специално обучение за всички изисквания и процедури за информационна сигурност, които се прилагат за защитата на данните и обработването на данни в рамките на техните индивидуални ежедневни роли и отговорности, включително докладване на нарушения на сигурността на личните данни.
7. Служителите получават обучение за обработване на жалби, свързани със защитата на данни и обработването на лични данни.
8. Директорът "Човешки ресурси" и Отговорникът по правни въпроси съхраняват документация за съответното обучение. За документиране на обучението по защита на личните данни се използва приложения по-долу формуляр:

ФОРМУЛЯР ЗА ПРОВЕДЕНО ОБУЧЕНИЕ ОТНОСНО ЗАЩИТАТА НА ДАННИТЕ

Име и Фамилия:

Позиция:

Отдел:

Моля опишете по какъв начин работата ви е свързана с обработването на лични данни:

(„обработване“ означава всяка операция или съвкупност от операции като събиране, записване, организиране, структуриране, съхранение, адаптиране или промяна, извличане, консултиране, употреба, разкриване, подреждане или комбиниране, ограничаване, изтриване или унищожаване)

Моля дайте оценка за проведеното обучение от 1 (най-неудовлетворително) до 5 (най-полезно).					
	1	**2**	**3**	**4**	**5**
Дали предостави необходимата информация?					
Дали информира служителите за задачите им, свързани с обработването на лични данни?					
Дали отговори на възникналите въпроси в достатъчна степен?					

Какви препоръки бихте направили във връзка с провеждане на обучението?