ПРОЕКТ!

КОДЕКС НА СЪЮЗ НА ВиК ОПЕРАТОРИТЕ В РЕПУБЛИКА БЪЛГАРИЯ ЗА ЗАЩИТА НА ЛИЧНИ ДАННИ

ВЪВЕДЕНИЕ :

Настоящият кодекс за поведение за защита на личните данни се приема на основание чл.40, §1 от 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 (по-нат. Регламента).

Кодексът съставлява ненормативен акт, съдържащ правила за поведение относно уточнение на прилагането на Регламента в областта на услугите по водоснабдяване, канализация, пречистване на питейните и отпадните води, които са нормативно регулирани, приет от сдружение Съюз на ВиК операторите в Република България и е одобрен от Комисия за защита на личните данни.

Сдружение Съюз на ВиК операторите в Република България (по – нат. „сдружението“) е сдружение с нестопанска цел, което обединява оператори на водоснабдителни и канализационни услуги по смисъла на Закон за регулиране на водоснабдителните и канализационни услуги (ЗРВКУ) при обработката на лични данни. По силата на чл.8 от Устава на сдружението, членове могат да бъдат само В и К оператори с основен предмет на дейност водоснабдяване, канализация, пречистване на питейни и отпадни води.

Настоящият кодекс съдържа утвърдени добри практики за обработка на лични данни от операторите на водоснабдителни и канализационни услуги и има характер на политика за обработка на данните от администраторите.

ГЛАВА ПЪРВА
Предмет и адресати

Чл.1. (1) Този кодекс урежда:

1. Принципите на добросъвестно и прозрачно обработване на лични данни от членовете на сдружението и от други администратори, които предоставят водоснабдителни и канализационни услуги;
2. Законните интереси на администраторите при обработване на лични данни за целите на предоставяне на водоснабдителни и канализационни услуги;
3. Редът, лицата и операциите по събиране на лични данни;
4. Псевдонимизацията, профилирането и автоматизирано вземане на решения при обработка на лични данни;
5. Дейностите и отговорностите по информиране на обществото и субектите на данните;
6. Начина на упражняване на правата на субектите на данни в областта на водоснабдителни и канализационни услуги;
7. Информирането и закрилата на децата и начина за получаване на съгласие от носещите родителска отговорност за детето;
8. Мерки и процедури за защита на данните и сигурността на обработването;
9. Процедури при нарушения на сигурността на лични данни от оператори на водоснабдителни и канализационни услуги;

10. Извънсъдебните производства и процедури за разрешаване на спорове между администраторите и субектите на данни;
11. Наблюдаващ орган за спазването на кодекса;
12. Присъединяване към кодекса от оператори на водоснабдителни и канализационни услуги;
13. Дейност на наблюдаващия орган по контрола за спазването на кодекса и съдействие на субектите на лични данни;
14. Последици от нарушенията на кодекса.

(2) Настоящият кодекс се прилага и е открит за присъединяване оператори на водоснабдителни и канализационни услуги.
(3) Кодексът се прилага само за дейности от оператори, извършващи водоснабдителни и канализационни услуги на територията на Република България.
(4) Кодексът може да се прилага и спрямо лица, които не членуват в сдружението, ако отговарят на определението на експлоатационните предприятия за водоснабдителни и канализационни услуги - "В и К оператори" по смисъла на чл.1, ал.1 от ЗРВКУ и са приели доброволно спазването и условията на наблюдаващия орган.

Чл.2. (1) Този кодекс цели осигуряване на най-висока степен на закрила на физическите лица във връзка с обработването на личните им данни, независимо от тяхното гражданство или местопребиваване относно кръга от дейности, извършвани от ВиК операторите.
(2) Въведените от кодекса правила имат действие на територията на цялата страна спрямо дейността на ВиК операторите, които са се присъединили към кодекса и гарантират минимални равни условия и гаранции за субектите на лични данни.
(3) Правилата на кодекса са съобразени с:

1. особеностите на дейността на Вик операторите, регулирана в ЗРВКУ, подзаконовите актове по прилагането му, актове на Комисия за енергийно и водно регулиране;
2. определените в действащото законодателство основания за обработване на лични данни;
3. правните и фактически особености на водоснабдителните и канализационните услуги, извършвани от експлоатационните предприятия за водоснабдителни и канализационни услуги;
4. законовите задължения за предаване на обработваните лични данни на трети лица – публични органи;
5. обработката на лични данни и защита на правото на неприкосновеност на личния живот в сектора на електронните комуникации;
6. дейностите и правомощията на наблюдаващия орган по спазването на кодекса.

Чл.3. (1) Приложението на настоящия кодекс е доброволно и поражда действие след акта за присъединяване към него от ВиК операторите.
(2) За лица, които не са присъединили към него, кодексът има информативен характер и необвързващо действие и не създава права или задължения за администраторите на лични данни.

Чл.4. Целите на уредба на настоящия кодекс са:

1. Създаване на еднообразни добри практики за защита на личните данни от Вик операторите;
2. Спазване от страна ВиК операторите на правото на ЕС и националното законодателство в областта на личните данни;
3. Практически гаранции относно задоволяване на правата и интересите на субектите на лични данни в качеството им на физически лица потребители по смисъла на §1, т.2 от ДР на ЗРВКУ ;
4. Въвеждане на национално приети правила за проследяване и контрол на режима на защита на личните данни чрез наблюдаващ орган;
5. Взаимодействие и методологично ръководство от страна на националния надзорен орган Комисия за защита на личните данни;
6. Облекчаване на административната тежест и процеса по отчетност на малките и средни предприятия относно въвеждане на режима на защита на личните данни.

Чл.5.(1) При приложението на настоящия кодекс членовете на сдружението и останалите ВиК оператори имат качеството на администратори на лични данни или на обработващи лични данни.
(2) Ако не е посочено друго, разпоредбите на Кодекса определят правата и задълженията на ВиК операторите като администратори на лични данни. В случаите, когато лицата имат качеството на обработващи лични данни са посочени изрично.
(3) ВиК операторите имат качеството на администратори на лични данни, когато обработката на лични данни е за изпълнение на дейността на администратора от тяхно име и за тяхна сметка, като вида на целите, средствата, данните, сроковете за съхранение и предаването на данните се определят от администратора, който контролира процесите по събиране и последваща обработка на данните, включително съвместно с други администратори или при възлагане на дейности на обработващи данните и по – специално дейността за предоставяне на ВиК услуги на потребители, дейността като работодател и възложител на доставката на стоки и услуги, включително по реда на Закон за обществените поръчки.
(4) В случаите, когато лицето има едновременно качество на обработващ и администратор на данните, при последваща промяна на целите и средствата на обработката, се прилагат отговорностите и санкциите като администратор на данни.
(5) Операторите са длъжни по прозрачен и разбираем за адресатите начин да предоставят недвусмислена информация дали действат в качеството на администратор или на обработващ, съответно за всички или за част от дейностите им.

ГЛАВА ВТОРА
РЕЖИМ НА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ
Раздел I.
Добросъвестно и прозрачно обработване на лични данни от ВиК операторите

Чл.6. ВиК операторите обработват лични данни при спазване на следните принципи:
1. законосъобразно, добросъвестно и по прозрачен начин обработване на данните;
2. обработване на ясно определен и ограничен обем от данни, пряко свързани с дейността по водоснабдителни и канализационни услуги;

3. мерки за осигуряване неприкосновеността на данните от неоправомощени по закон или договор трети лица;
4. точност и спазване на процедури за корекции на обработваните данни при грешки или непълнота;
5. съхранение на данните до определените в законодателството срокове и своевременно унищожаване на носителите на данни при спазване на правила за сигурност;
6. създаване на софтуерни продукти и носители на данни, които отговорят на изискванията за техническа защита на данните, прозрачност и проверка;
7. проследимост и механизъм за достъп до данните на субектите;
8. оценка на ниво на сигурност и на въздействието за личните данни и спазване на подходящи технически или организационни мерки за защита срещу неразрешено или незаконосъобразно обработване и срещу случайна загуба, унищожаване или повреждане на данните;
9. водеща роля на наблюдаващия орган за спазване и съдействие за изпълнението на мерките в кодекса;
10. въвеждане на изисквания, обучение и контрол върху дейността на служителите на администраторите за спазване на принципите чрез прилагане на мерките и документите, предвидени в този кодекс и указанията на наблюдаващия орган;
11. съответствие на административната тежест за малките и средни предприятия ВиК оператори с целите на защитата на личните данни.

Чл.7. (1) ВиК операторите обработват лични данни в един или повече от следните регистри:
1. Регистър на персонала на администратора относно данни на субектите по граждански и трудови договори;
2. Регистър на кандидати за работа по трудови и граждански договори;
3. Регистър на потребителите на ВиК услуги;
4. Регистър на контрагентите на администратора;
5. Регистър за видеонаблюдение и GPS проследяване;
6. Регистър на оплаквания на потребители;
7. Регистър на посетители.

(2) Всеки регистър съдържа данните, посочени в този кодекс, както и допълнителни данни, ако е необходимо. Администраторите имат право да определят други подходящи срокове за съхранение на данните, които отговарят на принципа за съответствие на срока с целите на обработката.
(3) Администраторите могат да водят и други, неизброени по – горе регистри, на дейностите по обработване при спазване на изискванията на Регламента за съдържанието на тези регистри.
(4) Администраторите определят вида на личните данни, целите и средствата за обработването им за отделните регистри, освен ако те не са определени със закон.

Чл.8. (1) **Регистър на персонала на администратора** съдържа следните данни, които се обработват с цел поддръжка на човешки ресурси за изпълнение на дейностите по занятие на администратора:

1. Данни за физическа идентичност на субектите – имена, ЕГН, адрес, телефон, месторождение, възраст, електронен адрес, документ за самоличност, саморъчен подпис;
2. Данни за социална и икономическа идентичност – трудовата дейност и образованието на субектите – стаж, предходни работодатели, образователни степени и институции, професионална квалификация, банкови сметки;
3. Данни за семейно положение – наличие на деца, сключен брак;
4. Данни за здравословното състояние на работници и служители и членове на семейството им;
5. Данни за придобита правоспособност и управление на МПС;
6. Други данни, определени от адмистратора.

(2) Данните по ал.1 се обработват на хартиен и/или електронен носител, като за част от данните има само запис на електронен носител без съхранение на документи, съдържащи данни.

(3) Данните се съхраняват на следните хартиени носители:

1. автобиография, мотивационно писмо, снимка, дипломи и други документи за доказване на професионална квалификация, трудов и граждански договори, длъжностна характеристика, допълнително споразумения към трудовия или граждански договор, актове за прекратяване на трудовото правоотношение, ведомости за изплатени възнаграждения, служебни бележки и удостоверения за трудов и осигурителен стаж и доходи, молби и заявления относно трудовото правоотношение (молби за ползване на отпуск, за напускане, за заместване, за трудоустрояване и други; декларации за получена трудова книжка, за удръжка от заплатата за допълнително пенсионно осигуряване; служебни бележки; протоколи за предадено материално оборудване и други, предвидени от Кодекс на труда и подзаконовите актове по прилагането му;

2. документ за медицински преглед при първоначално постъпване на работа и след преустановяване на трудовата дейност по трудово правоотношение за срок над 3 месеца по реда на Наредба № 4 от 11.05.1993 г. за документите, които са необходими за сключване на трудов договор; резултати от задължителни периодични медицински прегледи и изследвания по реда на Закона за здравословни и безопасни условия на труд и актовете по прилагането му; документи за медицинска екпертиза на работоспособността по смисъла на Наредба за медицинската експертиза.

(4) Част от изброените в ал.3 документи могат да бъдат създадени и обработвани в електронен вид.

(5) Данните по ал.1 се обработват със специализирани софтуерни програми за нуждите на начисляване и определяне на размера на трудови възнаграждения, определяне на размера на дължимите от осигурителя и осигурения осигуровки и данъци.

(6) Данните се обработват относно субекти, които са сключили трудов или граждански договор с администратора за нуждите на дейността му. Забрането е копирането на документи за самоличност и съхранение на копия от тях на хартиен или електронен носител за субектите, наети по трудови или граждански правоотношения.

(7) Данните се разкриват на законово основание на следните публични органи, въз основа на задължения в трудовото, данъчното и осигурителното законодателство:

1. Национална агенция за приходите;
2. Национален осигурителен институт;
3. Изпълнителна агенция „Главна инспекция по труда“.

(8) Данните по ал.1 относно идентификация на лицата от персонала на администратора не се публикуват на интернет страница или в други рекламни или промоционални без изричното съгласие на субектите.
(9) Данните по ал.1 на хартиен носител или под формата на записи на електронни носители се унищожават по предвидения в закона и този кодекс ред в следните срокове:

1. граждански договор, декларации относно осигуряване, хонорар - сметки – десет години след прекратяване на трудовото или гражданско правоотношение;
2. трудов договор, длъжностна характеристика, допълнителни споразумения, заповеди за ползван неплатен отпуск над 30 работни дни годишно, заповеди за прекратяване на трудовото правоотношение, ведомости за изплатени възнаграждения, декларации и удостоверения относно социално осигуряване по трудови правоотношения (обр. УП-1, обр. УП-2, обр. УП-3 и обр. 30) – 50 години от прекратяване на трудовото правоотношение;
3. всички останалали документи и записи, описани в ал.3 – според определени от администратора правила и изискванията на Закон за националния архивен фонд.

(10) По изключение посочените в ал.9, т.1 и т.3 срокове може да се удължат при наличие на образувани преди изтичане на срока на унищожаване на данните съдебни, административно-наказателни или административни производства и данните са необходими за провеждане на производствата. Администраторът определя само относими към характера на съответното производство данни, като останалите се унищожават.
(11) Точността и верността на данните се проверява от администратора чрез представени от субектите документи за самоличност, дипломи и други документи за квалификация, документи от медицинската експертиза, декларации и молби. При необходимост администраторът може да прави проверки до масиви от данни, които са публично достъпни по закон, справка за валидни документи за самоличност и др. Администраторът може да въведе задължения за наетите лица да декларират промени в данните в подходящ срок.
(12) Данните от регистър персонал се обработват от следните лица, определени от администратора:

1. законни представители на администратора по смисъла на приложимия към статута на лицето закон;
2. определени от него мениджъри човешки ресурси, специалисти личен състав, административни длъжности, счетоводители или други лица, наети по трудови правоотношения, с възложени функции по управление на хора според длъжността;
3. обработващи данни извън структурата на администратора, с които има сключен договор – счетоводни кантори и дружества за определяне на дължими трудови възнаграждения и свързани с тях публични плащания, одитори, посредници за наемане на работа, адвокати и адвокатски дружества.

(13) За данните от регистър персонал се прилагат правилата по-долу на кодекса относно:

1. права на субектите на данните;
2. задължения на обработващите на данни по договор с администратора;
3. технически и организационни мерки на защита на данните;
4. ред за унищожаване на данните;
5. информираност на субектите;
6. жалби и извънсъдебно разрешаване на спорове.

(14) Работодателят администратор въвежда процедура за контрол, достъп и докладване на нарушения на обработката на лични данни на работници и наети субекти по граждански договор по реда на този кодекс.
(15) Работодателят администратор въвежда системи за контрол на достъпа до помещенията, където се съхраняват и обработват данни, работно време на персонала и трудова дисциплина, които се съдържат в този кодекс и в правилниците за вътрешен ред.

Чл.9. (1) **Регистър на кандидати за работа по граждански и трудови договори** съдържа следните данни, които се обработват с цел осигуряване на персонал за изпълнение на дейностите по занятие на администратора:

1. Данни за физическа идентичност на субектите – имена, адрес, телефон, месторождение, възраст, електронен адрес, телефон, снимка, документ за самоличност;
2. идентичност – трудовата дейност и образованието на субектите – стаж, предходни работодатели, образователни степени и институции, професионална квалификация;
3. Данни за придобита правоспособност и специални умения – право на управление на МПС и др.;
4. други данни, определени от администратора.

(2) Данните по ал.1 се обработват на хартиен и/или електронен носител, като за част от данните има само запис на електронен носител без съхранение на документи, съдържащи данни. Данните се обработват със специализирани софтуерни продукти и автоматизирани системи, включително чрез попълване на въпросници и подаване на кандидатури онлайн.
(3) Данните се съхраняват на следните хартиени носители: автобиография, мотивационно писмо, снимка и други документи за доказване на професионална квалификация;
(4) Част от изброените в ал.3 документи могат да бъдат създадени и обработвани в електронен вид.
(5) Данните по ал.1 се обработват с цел подбор на квалифициран персонал, подходящ за осъществяване на трудовите функции или възложените работи.
(6) Данните се обработват относно субекти, които кандидатстват пряко или чрез посредници за сключване на трудови или граждански договори с администратора. Забрането е копирането на документи за самоличност и съхранение на копия от тях на хартиен или електронен носител за субектите, кандидати за работа.
(7) Данните се разкриват на законово основание на следните публични органи, въз основа на задължения в действащото законодателство:

1.органи на съд, прокуратура и МВР за нуждите на производства пред тях;
2. други контролни органи.

(8) Данните по ал.1 относно идентификация на кандидатите за работа не се публикуват на интернет страница или в други материали без изричното, съответно не се предават на други потенциални работодатели, без съгласие на субектите.
(9) Данните по ал.1 на хартиен носител или под формата на записи на електронни носители се унищожават по предвидения в закона и този кодекс ред в срок до шест месеца от представяне на кандидатурата за работа. За съхранение в по – дълъг срок се изисква съгласието на субектите.
(10) По изключение посочения в ал.9 срок може да се удължи при наличие на образувани преди изтичане на срока на унищожаване на данните съдебни, административно-

наказателни или административни производства и данните са необходими за провеждане на производствата. Администраторът определя само относими към характера на съответното производство данни, като останалите се унищожават.
(11) Точността и верността на данните се проверява от администратора чрез представени от субектите документи за самоличност, дипломи и други документи за квалификация, декларации и молби. При необходимост администраторът може да прави проверки до масиви от данни, които са публично достъпни по закон, справка за валидни документи за самоличност и др.
(12) Данните от регистър кандидати за работа се обработват от следните лица, определени от администратора:

1. законни представители на администратора по смисъла на приложимия към статута на лицето закон;
2. определени от него мениджъри човешки ресурси, счетоводители или други лица, наети по трудови правоотношения, с възложени функции по управление на хора според длъжността;
3. обработващи данни извън структурата на администратора, с които има сключен договор – посредници за наемане на работа, консултанти по управление на хора, адвокати и адвокатски дружества.

(13) За данните от регистър кандидати за работа се прилагат правилата по-долу на кодекса относно:

1. права на субектите на данните;
2. задължения на обработващите на данни по договор с администратора;
3. съгласие на субектите извън обхвата на данните, необходими за сключване на трудово или гражданско правоотношение;
4. технически и организационни мерки на защита на данните;
5. ред за унищожаване на данните;
6. информираност на субектите;
7. жалби и извънсъдебно разрешаване на спорове.

(14) Администраторът въвежда процедура за контрол, достъп и докладване на нарушения на обработката на лични данни на кандидати за наемане по трудови или граждански договор по реда на този кодекс.
(15) Администраторът въвежда системи за контрол на достъпа до помещенията и автоматизирани средства, където се съхраняват и обработват данни, работно време на персонала и трудова дисциплина, които се съдържат в този кодекс и в правилниците за вътрешен ред.

Чл.10. (1) **Регистър на потребителите на ВиК услуги** съдържа следните данни за физическа и икономическа идентичност на субектите – имена, ЕГН, адрес, телефон, факс, електронен адрес, вещни права върху недвижими имоти, документ за самоличност, саморъчен подпис и/или банкови сметки или други относими данни, определени от администратора.
(2) Данните по ал.1 се обработват на хартиен и/или електронен носител, като за част от данните има само запис на електронен носител без съхранение на документи, съдържащи данни.
(3) Данните се обработват с цел идентификация и сключване, изменение и прекратяване на договори с потребители на ВиК услуги за присъединяване и ползване на водоснабдителната

и канализационна мрежа и съоръжения; свързани с това услуги; изпълнение на изискванията на данъчното и счетоводното законодателство за отчетност, изискванията на Закон за устройството на територията и на Закон за водите.

(4) Данните се съхраняват на следните хартиени носители:

1. сключени договори, предварителни договори за присъединяване към водоснабдителната мрежа, допълнителни споразумения към тях; протоколи и приложения към договори; фактури, кредитни и дебитни известия и други;

2. заявление за присъединяване към водоснабдителната мрежа, заявления за откриване, промяна и прекратяване на партида, заявления за изграждане/подмяна/преместване на водоснабдителни и канализационни отклонения, заявки за спиране на водоподаване, заявки за съгласуване на проекти и предаване на изходни данни, заявление за предоставяне/прекратяване изпращане на електронни фактури, заявки за измерване на водонапор, декларации за собственост, съсобственост и титуляри наематели, заявления за издаване на становища, заявки за съгласуване на проекти, мрежи и съоръжения, заявления за предоставяне на ВиК данни, молби за проверки на измервателни средства, заявки за пломбиране, доставка и монтаж на водомери, заявки за анализи на питейна вода, жалби, сигнали и оплаквания на потребители и други документи относно договорите за предоставяне на ВиК услуги и други.

(5) Част от изброените в ал.4 документи могат да бъдат създадени и обработвани в електронен вид.

(6) Част от данните по ал.1 се обработват със специализирани софтуерни програми за управление на клиентски партиди, инкасо, системи за електронни плащания, счетоводни записвания, водене на счетоводни сметки, ДДС дневници, определяне на дължими данъци, архивиране на данни.

(7) Данните се обработват относно субекти, които са сключили договори за предоставяне на ВиК услуги с администратора и всички останали клиенти на администратора.

(8) Данните се разкриват на законово основание на следните публични органи, въз основа на задължения в данъчното, осигурителното законодателство и административното законодателство:

1. Комисия за енергийно и водно регулиране (КЕВР) на основание изискването на чл.17, ал.2 от ЗРВКУ за предаване на договорите с потребителите;

2. Национална агенция за приходите;

3. Национален осигурителен институт;

4. Държавна агенция „Национална сигурност“ относно мерки за изпиране на пари и предотвратяване на тероризма;

5. Агенция „Митници“ и икономическа полиция;

6. Други държавни и общински органи, сдружения на ВиК оператори.

(9) Лични данни, получени на основание сключените от администратора договори за предоставяне на ВиК услуги не се публикуват на интернет страница и/или в други рекламни или промоционални материали без изричното съгласие на субектите.

(10) Данните по ал.1 на хартиен носител и/или под формата на записи на електронен носител се унищожават по предвидения в закона и този кодекс ред в следните срокове:

1. договори за предоставяне на ВиК услуги и документи относно сключването, изпълнението и прекратяването им – десет години след прекратяване на договора;

2. всички останалали документи и записи, описани в ал.4 – според определени от администратора правила и изискванията на Закон за националния архивен фонд.

(11) По изключение посочените в ал.10, т.1 и т.2 срокове може да се удължат при наличие на образувани преди изтичане на срока на унищожаване на данните съдебни, административно - наказателни или административни производства и данните са необходими за провеждане на производствата. Администраторът определя само относими към характера на съответното производство данни, като останалите се унищожават.

(12) Точността и верността на данните се проверява от администратора чрез представени от субектите документи за самоличност, документи за наличие на вещни права върху недвижими имоти на основание чл.13, ал.2, т.4 и ал.3 от Наредба № 4 от 14.09.20104г. за условията и реда за присъединяване на потребителите и за ползване на водоснабдителните и канализационни системи, декларации, заявления и молби, удостоверения за банкови сметки от банки. При необходимост администраторът може да прави проверки до масиви от данни, които са публично достъпни по закон – справка в Имотен регистър, воден от Агенция по вписванията, справка за валидни документи за самоличност от интернет страницата на МВР, справки относно регистрани в Търговски регистър, воден от Агенция по вписванията, адреси за кореспонденция с НАП, телефони, факс и електронни адреси и др.

(13) Данните от регистър клиенти се обработват от следните лица, определени от администратора:

1. законни представители на търговеца по смисъла на приложимия към статута на лицето закон;
2. определени от него служители обслужване на клиенти, мениджъри, деловодители, счетоводители, юрисконсулти, мениджъри търговска дейност, търговски и финансови директори или други лица, наети по трудови правоотношения, с възложени функции по управление на договори с потребителите според длъжността;
3. обработващи данни извън структура на администратора, с които има сключен договор – счетоводни кантори и дружества за водене на счетоводни записи на доставените ВиК услуги и свързани с тях публични плащания, одитори, адвокати и адвокатски дружества, доставчици на платежни услуги, „Български пощи“ ЕАД дружества за събиране на вземания, застрахователни дружества, банки, консултанти и други, определени от администратора с нарочен договор.

(14) За данните от регистър потребители на ВиК услуги се прилагат правилата по-долу на кодекса относно:

1. права на субектите на данните;
2. задължения на обработващите на данни по договор с администратора;
3. съгласие и информираност на субектите;
4. технически и организационни мерки на защита на данните;
5. ред за унищожаване на данните;
6. жалби и извънсъдебно разрешаване на спорове.

(15) Забрането е копиране и съхранение на хартиен и/или електронен носител на документи за самоличност на лицата.

(16) Ползването на ЕГН на потребителите при възможност се заменя с посочване на абонатен/клиентски номер на лицата в договорите и другата съпътстваща документация. Последното не се прилага за сключвани договори, за които данъчното законодателство изисква подаване на декларации с посочване на ЕГН.

(17) Операторите приемат и съхраняват преписи от документи за наличие на право на собственост или на строеж или на други вещни права в предвидените в закона случаи (Чл.13, ал.2, т.4 и ал.3 от Наредба № 4 от 14.09.20104г. за условията и реда за присъединяване на потребителите и за ползване на водоснабдителните и канализационни системи). В тези случаи, операторите осигуряват подходящи технически и организационни мерки за съхранение на преписите от документи за наличие на вещни права (нотариални актове, договори за делба, заповеди, удостоверения за наследници, завещания и др.).

Чл.11. (1) **Регистър на контрагентите на администратора** съдържа следните данни за физическа и икономическа идентичност на субектите – имена, ЕГН, адрес, телефон, факс, електронен адрес, документ за самоличност, саморъчен подпис, банкови сметки или други данни, определени от администратора.
(2) Данните се обработват с цел доставка на стоки и услуги за извършване на присъщата дейност на администратора и за изпълнение на изискванията на данъчното и счетоводното законодателство за отчетност, включително изпълнение на процедури по Закон за обществените поръчки.
(3) Данните по ал.1 се обработват на хартиен или електронен носител, като за част от данните има само запис на електронен носител без съхранение на документи, съдържащи данни.
(4) Данните се съхраняват на следните хартиени или електронни носители:

1. сключени договори и допълнителни споразумения към тях; протоколи и приложения към договори; фактури, данъчни и кредитни известия;
2. уведомления, писма, документи за определяне на представители за нуждите на изпълнението на договорите, искови молби, заявления и други документи относно изпълнението на договорите;
3. заявления, спесификации, оферти, декларации, единен европейски документ за обществени поръчки (ЕЕДОП), искане за разяснения, жалби и други документи относно провеждане на обществени поръчки и приложени към тях доказателства относно кандидати и персонала им.

(5) Част от изброените в ал.4 документи могат да бъдат създадени и обработвани в електронен вид.
(6) Част от данните по ал.1 се обработват със специализирани софтуерни програми за счетоводни записвания, водене на счетоводни сметки, ДДС дневници, определяне на дължими данъци.
(7) Данните се обработват относно субекти, които доставят стоки и услуги за нуждите на дейността на администратора.
(8) Данните се разкриват на законово основание на следните публични органи, въз основа на задължения в данъчното, осигурителното законодателство и административното законодателство:

1. Национална агенция за приходите;
2. Национален осигурителен институт;
3. Държавна агенция „Национална сигурност“ относно мерки за изпиране на пари и предотвратяване на тероризма;
4. Агенция „Митници“ и икономическа полиция;
5. Агенция за обществени поръчки;
6. други държавни и общински органи.

(9) Лични данни, получени на основание сключени граждански и търговски сделки от администратора, не се публикуват на интернет страница или в други рекламни или промоционални материали без изричното съгласие на субектите.
(10) Данните по ал.1 на хартиен носител или под формата на записи на електронен носител се унищожават по предвидения в закона и този кодекс ред в следните срокове:
1. търговски и граждански договори и документи относно сключването, изпълнението и прекратяването им – пет години след прекратяване на търговското или гражданско правоотношение;
2. досиета относно процедури за провеждане на обществени поръчки – 5 години от датата на приключване изпълнението на договора за обществена поръчка или от датата на прекратяване на процедурата;
3. всички останалали документи и записи, описани в ал.3 – до две години след прекратяване на търговското или гражданско правоотношение.
(11) По изключение посочените в ал.10, т.1 - 3 срокове може да се удължат при наличие на образувани преди изтичане на срока на унищожаване на данните съдебни, административно - наказателни или административни производства и данните са необходими за провеждане на производствата. Администраторът определя само относими към характера на съответното производство данни, като останалите се унищожават.
(12) Точността и верността на данните се проверява от администратора чрез представени от субектите документи за самоличност, декларации и молби. При необходимост администраторът може да прави проверки до масиви от данни, които са публично достъпни по закон - справка за валидни документи за самоличност от интернет страницата на МВР, справки относно регистрани в Търговски регистър и Имотен регистър, водени от Агенция по вписванията, адреси за кореспонденция с НАП, регистър на публични задължения, Цетрален регистър на особените залози, телефони, факс и електронни адреси и др.
(13) Данните от регистър контрагенти се обработват от следните лица, определени от администратора:

1. законни представители на администратора по смисъла на приложимия към статута на лицето закон;
2. определени от него мениджъри обществени поръчки, счетоводители, юрисконсулти, мениджъри търговска дейност, търговски и финансови директори или други лица, наети по трудови правоотношения, с възложени функции по управление на хора според длъжността;
3. обработващи данни извън структура на администратора, с които има сключен договор – счетоводни кантори и дружества за определяне на дължими трудови възнаграждения и свързани с тях публични плащания, одитори, посредници за наемане на работа, адвокати и адвокатски дружества.

(14) За данните от регистър контрагенти се прилагат правилата по-долу на кодекса относно:

1. права на субектите на данните;
2. задължения на обработващите на данни по договор с администратора;
3. съгласие на субектите;
4. технически и организационни мерки на защита на данните;
5. ред за унищожаване на данните;
6. жалби и извънсъдебно разрешаване на спорове.

(15) Забрането е копиране и съхранение на хартиен или електронен носител на документи за самоличност на лицата, представляващи контрагентите.

Чл.12. (1) **Регистър видеонаблюдение и GPS проследяване** съдържа следните данни за физическа идентичност на субектите – образ, движения, филм, глас и снимка и местоположение по данни от GPS проследяване на служебни автомобили.
(2) Данните се обработват с цел защита на живота и здравето на лицата на служители и клиенти на администратора и запазване на имуществото на администратора.
(3) Данните по ал.1 се обработват с автоматизирани системи със или без съхранение на записи и без съхранение на документи, съдържащи данни, на основане чл.22, ал.2 от Закон за частната охранителна дейност за нуждите на самоохрана на помещенията на администратора или по договор с изпълнител на дейности по охрана по смисъла на чл.56, ал.1, т.1, б.“в“ от Закон за частната охранителна дейност.
(4) Данните се съхраняват на следните електронни носители:

1. Сървър с данни в електронен формат;
2. Други технически носители – дискове, хард драйвъри, флаш памет и т.н.

(5) На обектите (сгради, стопански дворове, складове, съоръжения за води, автомобили), офисите за прием на потребители и вътрешни помещенията на администратора се поставя обозначителен надпис за извършване на видеонаблюдението или GPS проследяване, който е ясно разпознаваем около входа, за да може субектите да преценят дали да влязат в обекта или помещенията или автомобилите. Във всяко от помещенията се поставя знак за осъществявано видеонаблюдение.
(6) Администраторът определя в кои от помещенията му ще се извършва видеонаблюдение съответно на необходимостта от охрана на имуществото и персонала на администратора. Забранява се поставянето на видеонаблюдение в сервизните и санитарни помещения, както и видеонаблюдение на пространства на публични обществени места извън границите на имотите на администратора.
(7) Средствата за видеонаблюдение се описват, преди поставянето им в действие, като се посочва модел, номер, функционалност (приемане на образ и звук, само на образ; резолюция; възможност за възпроизвеждане на образ и/или звук или снимка; нощен режим на работа).
(8) Данните се обработват относно субекти, които се намират в обектите и помещенията на администратора – потребители, контрагенти, други външни лица и персонал на администратора. Данните се обработват и за водачите на служебни автомобили на администраторите по време на изпълнение на служебни задължения.
(9) Наблюдаваните лица имат право на преглед на записите, ако се съхраняват такива. Правото се осъществява по реда на кодекса и при предварително обособяване от страна на администратора на части от записа, като се избягва предоставянето на запис относно наблюдение на други субекти без присъствие в кадъра на субекта.
(10) Данните се разкриват на законово основание на следните публични органи, въз основа на задължения в действащото законодателство:

1. органите на МВР и на Държавна агенция "Национална сигурност" за извършено, извършвано или подготвяно престъпление или нарушение на обществения ред, незабавно след узнаването ѝ и/или при поискване от съответните длъжностни лица по реда на Закона за Министерството на вътрешните работи и Закона за Държавна агенция "Национална сигурност" на основание чл.54, ал.1 от ЗЧОД;
2. Органите на прокуратура и съд въз основа на предвидени в наказателно процесуалното право задължения и законни разпореждания на посочените органи.

(11) Лични данни, получени на основание видеонаблюдение и GPS проследяване, не се публикуват и не се предават на трети лица, извън посочените в ал.10.
(12) В случай на извършване на видеонаблюдение по договор с изпълнител на охранителна дейност по смисъла на ЗЧОД, администраторът изисква от изпълнителя изпълнението на задълженията по законодателството в областта на личните данни и в ЗЧОД относно водене на регистри за видеонаблюдение на охранявани обекти, включително срокове за съхранение.
(13) Данните по ал.1 под формата на записи в автоматизирани системи се унищожават по предвидения в закона и този кодекс ред след изтичане на 30 дни от извършеното наблюдение. За данни от GPS проследяване администраторите могат да определят по – дълъг срок.
(14) Срокът по ал.13 не може да се удължава.
(15) Точността и верността на данните се проверява от администратора чрез представени от доставчиците или от изпълнителите на охранителна дейност документи за изправността и функционалността на средствата за видеонаблюдение и за възможностите им за предаване и съхранение на данните.
(16) Данните от регистър видеонаблюдение се обработват от следните лица, определени от администратора:

1. законни представители на търговеца по смисъла на приложимия към статута на лицето закон;
2. определени от него лица за осигуряване на самоохрана на помещенията на администратора;
3. обработващи данни извън структура на администратора, с които има сключен договор – изпълнителни на частна охранителна дейност, получили лиценз за частна охранителна дейност по реда на ЗЧОД.

(17) За данните от регистър видеонаблюдение се прилагат правилата по-долу на кодекса относно:

1. права на субектите на данните;
2. задължения на обработващите на данни по договор с администратора;
3. съгласие на субектите;
4. технически и организационни мерки на защита на данните;
5. ред за унищожаване на данните;
6. жалби и извънсъдебно разрешаване на спорове.

Чл.13. (1) **Регистър на** клиенти на администратора на **оплаквания на потребители** съдържа следните данни :

1. физическа идентичност на субектите – имена, адрес, телефон, електронен адрес, саморъчен/електронен подпис;
2. други данни, определени от администратора.

(2) Данните се обработват с цел изпълнение на нормативните изисквания на Наредба за регулиране на качеството на водоснабдителните и канализационни услуги, която изисква да се води статистика и да се регистрират всички оплаквания на потребители относно качеството на ВиК услугите. По смисъла на §1, т.10 от Наредба за регулиране на качеството на водоснабдителните и канализационни услуги, оплакване на потребител съставляват жалби, сигнали и молби от потребители във формата на писмен документ, включително писмо, бележка, заявление или друга форма на писмена комуникация, подадени директно в

дружеството или по електронен път, лицензиран пощенски оператор, факс или по друг технически възможен начин, отнасящи се до услуга или действие на В и К оператора или негови представители, в които са изложени твърдения, че не отговарят на нормативно определените изисквания за предоставяните услуги и/или се нарушават търговските отношения между страните.

(3) Данните по ал.1 се обработват на хартиен или електронен носител, записи в автоматизирани системи, попълване на данни онлайн и автоматизирани системи.

(4) Данните се съхраняват на следните хартиени или електронни носители:

1. писмен документ, включително писмо, бележка, заявление или друга форма на писмена комуникация;

2. отговори, решения, заповеди, декларации и протоколи във връзка с извършените действия по разглеждане на оплакването.

(5) Част от изброените в ал.4 документи могат да бъдат създадени и обработвани в електронен вид, включително чрез онлайн автоматизирани системи за обработване.

(6) Част от данните по ал.1 се обработват със специализирани софтуерни програми за водене на деловоден регистър на оплакванията. Програмите отговорят на изискванията за автоматизирано обработване на данни в този кодекс и в закона.

(7) Данните се обработват относно субекти, които са потребители на администратора, подали оплаквания.

(8) Данните не се разкриват регулярно на законово основание на публични органи или на други трети лица, освен в предвидените в закона случаи на КЕВР в производствата по оценка на качеството на услугите.

(9) Лични данни, получени на основание оплаквания на потребители, не се публикуват на интернет страница на администратора без изричното съгласие на субектите.

(10) Данните по ал.1 на хартиен носител или под формата на записи в автоматизирани системи се унищожават по предвидения в закона и този кодекс ред в срок от пет години от получаване на оплакването.

(11) По изключение посочения в ал.10 срок може да се удължи при наличие на образувани преди изтичане на срока на унищожаване на данните съдебни, административно - наказателни или административни производства и данните са необходими за провеждане на производствата. Администраторът определя само относими към характера на съответното производство данни, като останалите се унищожават.

(12) Точността и верността на данните се проверява от администратора чрез представени от потребителите документи за измервания, протоколи, документи за самоличност, декларации и молби. При необходимост администраторът може да прави проверки до масиви от данни, които са публично достъпни по закон - справка за валидни документи за самоличност от интернет страницата на МВР и др.

(13) Данните от регистър на оплакванията се обработват от следните лица, определени от администратора:

1. законни представители на администратора по смисъла на приложимия към статута на лицето закон;

2. определени от него директори и експерти по качеството, мениджъри търговска дейност, търговски и финансови директори или други лица, наети по трудови правоотношения, с възложени функции по управление на качеството на услугите според длъжността;

3. обработващи данни извън структура на администратора, с които има сключен договор –консултанти по управление на качеството.

(14) За данните от регистър на оплакванията се прилагат правилата по-долу на кодекса относно:

1. права на субектите на данните;
2. задължения на обработващите на данни по договор с администратора;
3. съгласие на субектите;
4. изисквания за обработване на лични данни на деца;
5. профилиране и автоматизирано обработване на данни;
6. технически и организационни мерки на защита на данните;
7. ред за унищожаване на данните;
8. жалби и извънсъдебно разрешаване на спорове.

(15) Забрането е копиране и съхранение на хартиен или електронен носител на документи за самоличност на клиентите на администратора.

(16) Ползването на ЕГН на клиентите, се заменя преимуществено с посочване на абонатен номер в оплакванията и съпътстващата документация.

Чл.14. (1) **Регистър на посетителите** съдържа следните данни : физическа идентичност на субектите – имена и/или документ за самоличност.

(2) Данните се обработват с цел контрол на достъпа до служебни помещения за осъществяване на дейността му и защита на имуществото, персонала и личните данни.

(3) Данните по ал.1 се обработват на хартиен или електронен носител.

(4) Данните се съхраняват на следните хартиени или електронни носители: дневник на посетители.

(5) Данните се обработват относно субекти, които посещават и имат достъп до помещенията и имотите на администратора, с изключение на публично достъпните офиси за работа с потребители и доставчици на стоки и услуги.

(6) Данните не се разкриват регулярно на законово основание на публични органи или на други трети лица, освен в предвидените в закона случаи.

(7) Данните по ал.1 на хартиен носител или електронен носител се унищожават по предвидения в закона и този кодекс ред в срок от една година от завеждане на посещенията.

(8) По изключение посочения в ал. 7 срок може да се удължи при наличие на образувани преди изтичане на срока на унищожаване на данните съдебни, административно - наказателни или административни производства и данните са необходими за провеждане на производствата. Администраторът определя само относими към характера на съответното производство данни, като останалите се унищожават.

(9) Точността и верността на данните се проверява от администратора чрез представени от субектите документи за самоличност.

(10) Данните от **регистър на посетителите** се обработват от следните лица, определени от администратора:

1. законни представители на администратора по смисъла на приложимия към статута на лицето закон;
2. определени от него охранители или други лица, наети по трудови правоотношения, с възложени функции по контрол на достъпа според длъжността.

(11) За данните от **регистър па посетителите** се прилагат правилата по-долу на кодекса относно:

1. права на субектите на данните;
2. задължения на обработващите на данни по договор с администратора;
3. съгласие на субектите;
4. изисквания за обработване на лични данни на деца;
5. технически и организационни мерки на защита на данните;
6. ред за унищожаване на данните;
7. жалби и извънсъдебно разрешаване на спорове.

(12) Забрането е копиране, сканиране и съхранение на хартиен или електронен носител на документи за самоличност на посетителите.

Чл.15. (1) Администраторите определят кои от изброените в чл.7, ал.1 регистри водят и се задължават да спазват посочените изисквания за добросъвестно и прозрачно обработванте на данните.
(2) При наличие на регистър, който не попада в посочените, администраторите водят допълнително неоходимата отчетност в пределите, определени за изброените в кодекса регистри.

Чл.16. (1) Администраторите се придържат към принципа за минимално обработване на лични данни. Ако се обработват данни, извън изброените в Кодекса за всеки вид регистър, администраторът следва да мотивира по каква причина обработва данни извън изброените в кодекса.
(2) За всеки от регистрите се посочва началната и крайната дата на водене на съответния регистър, както и наименованието и координатите за връзка на администратора, и когато е приложимо, на съвместните администратори и на длъжностното лице по защитата на данните.
(3) Данните относно водените регистри се съхраняват в писмена форма, включително в електронен формат.
(4) Администраторите имат право да регулират съобразно особеностите на дейността им елементи от водените регистри по начин, различен от описания в кодекса (обработващи, срокове за съхранение на данните и др.).

Чл.17.(1) Данните в регистрите, включително допълнително създадените такива извън предвидените по – горе, се обработват на едно или повече от следните правни основания по смисъла на Регламента :

1. Сключен договор за ВиК услуги с потребители на основание чл.14 от Наредба № 4 от 14.09.2004г. за условията и реда за присъединяване на потребителите и за ползване на водоснабдителните и канализационни системи; трудови и граждански договори; договор за изпълнение на обществени поръчки, други договори, включително дистанционно при спазване на изискванията за предоставяне на информация чрез комуникационни технологии;
2. Съгласие на субектите, предоставено конкретно относно определена ясно цел, с точно посочване на обхвата на данните и останалата информация по Регламента, като съгласието може да бъде предоставени по един от следните начини :
   - С писмена декларация или декларация, попълнена онлайн от субекта и подписана с електронен подпис;

- Електронна форма на декларация, която се генерира автоматично от интернет страница или друга автоматизирана система за обработка на данните, която се съхранява трайно и изисква изрично потвърждение от страна на субекта с отбелязване в диалогови прозорци.

3. за изпълнение на легитимни интереси на администратора или на трета страна – ясно посочване за субектите на интересите и разграничение от случаите на предвидено в нормативен източник основание за обработка на данните;
4. изпълнение на нормативни изисквания за обработка на данни.

(2) В случаите по ал.1, т.2 съгласието се изисква преди обработката на данни от субекта, включително с автоматизирани системи, като ясно се разделя от други декрации и данни и се предоставя необходимата информация относно обработването. Системата ясно посочва на субекта, че липсата на съгласие е препятствие за продължаване на операциите в информационната и комуникационна среда, единствено, ако данните са пряко относими към предоставянето на услугата и няма друго основание за обработка на данните, което не изисква съгласие.

Чл.18.(1) Обработването на специални категории данни по чл.9 от Регламента се извършва при наличие на едно или повече от следните основания :

1. изрично съгласие – писмения документ или софтуерният продукт под формата на автоматично генерирани декларации да предоставят ясна информация на субекта за обстоятелството, че данните са специални ведно с изискуемите други данни по Регламента за съгласието;
2. изпълнението на задълженията и упражняването на права на администратора или на субекта на данните по силата на трудовото, осигурителното или данъчното законодателство или законодателството в областта на водоснабдителните и канализационни услуги - ясно посочване на съответните правни норми или на колективния трудов договор, по силата на които се събират данните;
3. защитени жизненоважните интереси на субекта на данните или на друго физическо лице – посочване на точните интереси, както и дали невъзможността за предоставяне на съгласие от субекта се дължи на правна или фактическа невъзможност;
4. публично оповестени от субекта данни – възможност за недвусмислено доказване на източника, включително при системи за каталогизиране на данни в интернет при спазване на принципа за пропорционалност на обработката във времето;
5. цел установяване, упражняване или защита на правни претенции - да се предоставя ясна информация за конкретния правен спор или правоотношение, съдържанието на което е свързано с правния спор;
6. причини от важен обществен интерес на основание правото на Съюза или българското право – ясно определяне на правните норми, вида на интереса и пропорционалността на защитата (организационни и технически мерки на закрила, срок на обработката и т.н.).

(2) Обработката на ЕГН или други национални идентификационни номера на потребителите се извършва само при правно основание или при доказана липса на друг начин за достоверно индивидуализиране на субекта при наличие на някое от основанията по – горе.

(3) Обработването на личните данни на наетите лица по трудово ли служебно правоотношение следва да отговарят на изискванията на приложимото трудово или

административно законодателство относно обхвата на данните и начините на обработването, включително специалните изисквания за закрила на данните.

Раздел II.
Законни интереси за обработка на лични данни на доставчиците на водоснабдителни и канализационни услуги

Чл.19. (1) Всяко обработване на лични данни по реда на кодекса е в изпълнение на законни интереси на администратора по смисъла на правото на ЕС или на вътрешните източници на българското право.
(2) При отпадане на законния интерес от обработване на данните, администраторът спира дейностите от деня на отпадане на интереса. Счита се, че интересът е отпаднал в следните случаи:

1. вземане на решение за прекратяване дейността на търговеца, откриване на производство по ликвидация или несъстоятелност – всички регистри;
2. прехвърляне на търговско предприятие или на обособена част от него;
3. прекратяване на разрешение или лицензия за извършване на правно регламентирана дейност;
4. изтичане на сроковете за обработка на данните;
5. прекратяване на сключени договори за обработка на данни, независимо от основанието;
6. прекратяване на сключен договор за охрана относно регистъра за видеонаблюдение.

(3) Администраторът временно преустановява водените регистри при спиране дейността на предприятието или поради неизпълнение на определените в закон изисквания, които временно препятстват дейността.
(4) При спиране на обработването, администраторът определя със заповед лица, които отговарят за архивиране и спазване на сроковете за унищожаване на данните.
(5) При временно преустановяване обработването на данни, администраторът взема предвидените организационни и технически мерки за архивиране и съхранение на данните.
(6) Администраторът въвежда подходящи технически мерки за автоматизирано съхранение (бек - ъп) на данните при спиране или преустановяване на обработката с функционалностите за търсене и възстановяване на данните при конфигуриране на достъпа без преинсталация и проследимост на логовете за дезархивиране (пароли за достъп, обхват на дезархивираната информация и др.).

Чл.20.Всяко предаване на лични данни от администратора на трети лица се основава на законен интерес, описан в настоящия кодекс или в действащото законодателство.

Чл.21.(1) Обработването на данните може да бъде ограничено при оспорване на точността на личните данни от субекта на данните и тяхната точност или неточност не може да бъде проверена, личните данни трябва да бъдат запазени за доказателствени цели или по разпореждане на Комисията.
(2) Софтуерните продукти или системи за автоматизирана обработка на данните при възможност следва да осигуряват функционалности за клиентите за проверка на точността

на данни от публични източници или при специален достъп, предоставен от публични органи.
(3) Администраторът информира субекта на данните преди да премахне ограничаването на обработването, когато то е наложено при оспорване на точността им.
(4) В ползваните от администраторите автоматизирани регистри на личните данни ограничаването на обработването се осигурява чрез техническа забрана за корекции или промяна на въведените данни чрез последващи операции.
(5) Обработване на данните от различните регистри за цели, различни от тези, описани в кодекса, не се допуска, освен за изпълнението на задача от обществен интерес и предвидените в действащото законодателство изключения.
(6) Софтуерните продукти или системи за автоматизирана обработка на данните следва да забранят въвеждане и съхранение на данни, извън определените за конкретния регистър и конкретните цели.

Чл.22. (1) Преди събиране на данните на субектите се предоставя информацията по чл.13 от Регламента в устна или писмена форма
(2) На интернет страницата на администратора и/или на видно място в помещенията на обектите за извършване на търговска дейност с потребители се поставя информация за вида на обработваните данни на законово основание, цели и описание, че данните се предават на трети лица – КЕВР, НАП, НОИ, лицензирани изпълнители на охранителна дейност и други органи за контрол на дейностите в областта на ВиК услугите. Допустимо е да не се предоставя индивидуално информация по чл.13 от Регламента при всяка сделка или обработка на данни, ако информацията се съдържа в публикуваната политика за конфиденциалност и субектът може да се запознае с нея преди предоставяне на данните по подходящ начин, съответно в документите има изрично отпращане към източника на публикацията на политиката, както и когато субектът вече разполага с информацията.
(3) Извън случаите на предоставяне на ВиК услуги, администраторът може да изисква доказателства за запознаване на субекта с информацията по чл.13 от Регламента под формата на писмена декларация, електронно съобщение, кратко текстово съобщение, автоматично генерирани диалогови прозорци от софтуерни продукти или автоматично генерирани диалогови прозорци и съобщения на интернет страници. Субектът не може да бъде задължен да потвърди информираността си като основание за предоставяне на услуги, като формата следва да предоставя възможност за отказ за запознаване с информацията.
(4) За регистрите по чл.7, ал.2 преди обработване на данните се предоставя в устна или писмена форма информацията по чл.13 от Регламента.
(5) За регистъра по чл.7, ал.2, т.5 информацията се предоставя чрез поставеното обявление за наличието на видеонаблюдение в помещенията и на МПС или чрез друго информационно табло при необходимост.

Чл.23.(1) При обработка на данни, които не са получени от субекта, преди обработката се предоставя информацията по чл.14 от Регламента.
(2) На интернет страницата на администратора и/или на видно място в помещенията на обектите за извършване на търговска дейност се поставя информация за вида на обработваните данни на законово основание, цели и описание, че данните се предават на трети лица – НАП, НОИ, лицензирани изпълнители на охранителна дейност и други органи за контрол на дейностите в областта на ВиК услуги. Допустимо е да не се предоставя

индивидуално информация по чл.14 от Регламента при всяка сделка или обработка на данни, ако информацията се съдържа в публикуваната политика за конфиденциалност и субектът може да се запознае с нея преди предоставяне на данните по подходящ начин, съответно в документите има изрично отпращане към източника на публикацията на политиката, както и когато субектът вече разполага с информацията.
(3) При обработка с автоматизирани системи, допустимо е информацията по чл.14 да се изпраща чрез автоматизирано генерирани електронни съобщения или кратки текстови съобщения.

Чл.24.(1) При обработката на данни администраторът осигурява изпълнението на изискванията на правото на ЕС в областта на обработката на лични данни и защита на правото на неприкосновеност на личния живот в сектора на електронните комуникации (Директива 2002/58/ЕО относно за правото на неприкосновеност на личния живот и електронни комуникации).
(2) Изискванията на защитата на неприкосновеността в електронните комуникации се отнася до :
1. подходящи средства за информиране на субектите относно обработването на данните;
2. ползването на данни относно трафик и местонаходение на субектите, движение в пространството, онлайн идентификатори и други данни, придобите чрез съобщенията и свързания трафик на данни през публични комуникационни мрежи и публично достъпни електронни комуникационни услуги;
3. информация за нарушение на сигурността на мрежата и процедури за уведомяване на абонатите относно рисковете;
4. мерки за осигуряване на защита и конфиденциалност на информацията, обработвана чрез публични комуникационни мрежи и публично достъпни електронни комуникационни услуги;
5. предоставяне на ясна и цялостна информация при използването на електронни комуникационни мрежи, за да се съхранява информация или да се получи достъп до информация, съхранявана в терминалното оборудване на абоната или потребителя.

Чл.25.(1) При обработка на данни, съхранявани в терминалното оборудване на субекта, предварително се предоставя информацията по чл.22 по – горе относно вида и обхвата на данните, които се придобиват от терминалното устройство, съответно законното основание за обработката на данните.
(2) Ако се изисква съгласието на субектите за обработката на данни, то трябва да се изиска и предостави преди да е осъществен достъпа до данните в терминалното устройство.
(3) Правилата за предоставяне на информация и съгласие не се прилагат, ако техническото съхранение или достъп са с единствена цел осъществяване или улесняване на предаването на комуникация през електронна комуникационна мрежа или като точно необходима, за да се предостави информационна обществена услуга, изрично поискана от субекта.
(4) Ползването на софтуер за наблюдение, снифери, скрити идентификатори и други подобни устройства, които имат достъп до терминала на субектите без тяхното знание, за да получат достъп до информация, да съхраняват скрита информация или да проследяват действията на потребителя се извършва позволено само за законни цели със знанието на заинтересованите субекти.

(5) Автоматизираната обработка на данни или профилиране чрез кукита (cookies) е легитимна при анализиране на ефективността на дизайна на интернет страницата и рекламиране и проверка идентичността на субекта, ангажиран в сделки онлайн, за улесненение на осигуряването на услуги за информационно общество.
(6) Интернет страницата следва да предоставя предварително на субектите точна и ясна информация относно вида кукита, данните, което се обработват от кукитата, целите, както и останалата информация по Регламента.
(7) Преди осъществяване на технически достъп до данитте от терминалното устройство, субектите трябва да имат възможност да откажат да достъпа на куки или на други подобни приспособления, имащи достъп до тяхното терминално оборудване, освен ако кукита не са необходими за изпълнението на услугата.
(8) Информацията и правото на отказ могат да бъдат предложени веднъж за използване на различни приспособления, които ще се инсталират на терминалното оборудване на потребителя по време на същото включване, и също така обхващащи бъдещо използване, което може да се направи за тези услуги по време на следващи включвания. Начинът на предоставяне на информацията следва да бъде под формата на диалогови прозорци, падащи интерактивни съобщения и други подходящи технически решения, като методите за даване на информация, предлагаща право на отказ, или изискваща съгласие, трябва да са възможно най-лесни за ползване от потребителя.
(9) Приспособленията трябва да имат техническа възвожност за външна проверка от трето лице на вида на събираните данни, логовете и съхранението им, за да се гарантира, че не се събират данни от терминалните устройства, извън обявените такива.
(10) Администраторът следва да осигури възможност за субекта да има достъп до интернет страницата или услугата без обработката на данни от кукита, освен ако това е необходимо за самото естество на услугата, изисващо определена идентификацията на потребителя.

Чл.26. (1) При обработване на данни от трафик и/или онлайн идентификатори, субектът следва да бъде предварително информиран относно вида на данните и обработката им по смисъла на чл.13 от Регламента, маркетингови дейности или профилиране, съответно да му бъде поискано съгласието за тази обработка и гарантирано правото на оттегляне на съгласието и изтриване на данните чрез облекчени технически средства и по всяко време.
(2) Администраторът и обработващия следва да поддържат подходящи записи и доказателства за автоматизираното предоставяне на информация и съгласие от субектите за обработка на данни от трафик.

Раздел III .
Събиране на данните и псевдонимизация

Чл.27. (1) Събирането на данните е първоначално или последващо.
(2) Първоначалното събиране на данни се осъществява при извършване на съответната операция – преди сключване на договор с потребител на ВиК услуги, сключване на договор за трудово или гражданско правоотношение със субектите от персонала на администратора, преди сключване на търговска сделка с контрагенти, при искане за участие в промоционални или маркетингови дейности и други.
(3) При последващото събиране на данни се извършва обработка на нови видове данни при вече възникнали правоотношения.

(4) Администраторът следва да информира субекта за последващо събиране на данни съобразно изискванията на чл.13 и чл.14 от Регламента.

Чл.28. (1) Данните се събират пряко от субектите чрез предоставените от тях устно или в писмена форма, включително чрез автоматизирани системи, данни.
(2) Информацията се събира от субектите и по електронен път, включително чрез електронна поща. В случай, че информацията се попълва и подава чрез готови бланки чрез интернет страницата на администратора или трето лице, подадените данни се съхраняват по реда на посочените в кодекса мерки на техническа защита.

Чл.29. (1) Данните се събират само от изрично определените от администратора служители и обработващи данни.
(2) Лицата са длъжни да ползват личните данни от само, ако имат право на това според конкретно възложените трудови функции или възложена работа и според правилата на кодекса за персонална защита.
(3) Лицата ползват само личните данни, до които имат право на законосъобразен достъп и когато са им необходими във връзка с изпълнението на конкретните служебни задължения, като спазват приетите технически и организационни мерки, включително и специално, ако данните се предават по електронен път, за защитата им от случайно или незаконно нарушение, незаконно разкриване или достъп, нерегламентирано изменение или разпространение, както и всички други форми на обработване на личните данни.
(4) Лицата са длъжни да събират, обработват и съхраняват личните данни в регистрите така, че да предотвратяват тяхното разпространение или узнаване от трети лица.
(5) Всички лични данни от регистрите, които стават достъпни на лицата или по повод на изпълнение на техните задължения, са конфиденциални. Лицата нямат право да разпространяват под каквато и да е форма и пред когото и да е факти и сведения, които представляват лични данни и са узнати от него при и по повод изпълнение на служебните задължения.
(6) Лицата нямат право, извън уреденото със законово основание или по изрично нареждане на администратора, да копират, преглеждат, изнасят на материални носители, включително електронни, да изпращат по електронен път или по друг начин лични данни, до които имат достъп при изпълнение на служебните си задължения.
(7) Администраторът предвижда изрична дисциплинарна отговорност за нарушение на трудовата дисциплина в трудовите договори, правилника за вътрешен трудов ред и/или длъжностните характеристики на служителите при нарушение на задълженията им по кодекса и актовете по прилагането му в предприятието на администратора.

Чл.30. (1) Обработването на лични данни от обработващи се извършва при спазване на изискванията на Регламента и на Закона за защита на личните данни. Операторите определят един или повече от следните обработващи според предмета на дейността :

1. доставчици на счетоводни, одиторски и юридически услуги;
2. доставчици на специализиран софтуер за управление на счетоводни, деловодни данни и данни на потребители на ВиК услуги;
3. лицензирани изпълнители на охранителни дейности;
4. доставчици на платежни услуги;
5. доставчици на универсални пощенски и куриерски услуги;

6. дружества за събиране на вземания;
7. доставчици на строителни и проектантски услуги;
8. други видове обработващи данни, определени от администратора.

(2) Администраторът определя обхвата на данните и задълженията на обработващите в договор или друг акт, в който регламентира предмета и срока на действие на обработването, естеството и целта на обработването, вида лични данни и категориите субекти на данни и задълженията и правата на администратора, както и останалата информация по чл.28, §3 от Регламента.

(3) В договора или друг акт изрично се определят данните от кои регистри по смисъла на този кодекс се обработват и се възлага спазването на всички правила на този кодекс, включително технически и организационни мерки при обработването.

(4) Позоваването на настоящия кодекс в договорите с обработващи е доказателство за предоставянето на достатъчни гаранции от обработващите по смисъла на чл.28, §1 и §4 от Регламента.

(5) Наблюдаващият орган може да приеме стандартни клаузи за договорите с обработващи данни, които се включват в тях.

(6) Обработващият няма право да изготвя и съхранява копия от носители, съдържащи обработените лични данни, след като оргиналите бъдат предадени на администратора.

(7) Обработващият няма право да дава информация или да предоставя достъп до обработваните данни на други обработващи или на трети лица без получаване на предварителното разрешение от страна на администратора.

(8) Всички лични данни от регистрите, които стават достъпни на обработващия при или по повод изпълнение на неговите задължения са конфиденциални.

(9) Обработващият не може да разпостранява под каквато и да форма и пред когото и да е факти, които представляват лични данни и са узнати от него при или по повод изпълнението на задължението му.

(10) Ако обработващ лични данни определи в нарушение на правилата на закона или кодекса целите и средствата на обработването, обработващият личните данни се счита за администратор по отношение на това обработване.

(11) Обработващият лични данни и всяко лице, действащо под ръководството на администратора или на обработващия лични данни, което има достъп до личните данни, обработва тези данни само по указание на администратора, освен ако обработването се изисква от правото на Европейския съюз или законодателството на Република България.

(12) В договорите с обработващите администраторите следва да предвидят задължения за обработващите да съдействат на наблюдаващия кодекса орган да осъществи контрол върху изпълнението на задълженията на обработващите.

Чл.31. (1) Събирането на лични данни се подчинява на правилата за отчетност, съответно събиране само на данни и по начин, описан в регистрите по кодекса.

(2) Обработването на данни чрез въведените автоматизирани системи се извършва при спазване на изискванията на закона относно наличието на записи (логове) най-малко за следните операции по обработване: събиране, промяна, справки, разкриване, включително предаване, комбиниране и изтриване.

(3) Записите за извършена справка или разкриване трябва да дават възможност за установяване на основанието, датата и часа на такива операции и доколкото е възможно —

идентификацията на лицето, което е направило справка или е разкрило лични данни, както и данни, идентифициращи получателите на тези лични данни.
(4) Записите се съхраняват в определените в кодекса срокове.

Чл.32. (1) Администраторите полагат усилия за въвеждане на псевдонимизация на личните данни във всички регистри, в който това е допустимо. Въвеждането на псевдонимизацията се основава на посочените по – долу насоки, ако администраторът притежава технически и организационни възможности за това.
(2) Псевдонимизацията на данните се извършва при спазване на следните принципи:
1. операциите се извършват на най-ранния възможен етап на обработка на данните – при създаване на партида на потребител при обработка на заявление за присъединяване към водопреносната мрежа или други услуги;
2. съответствието между оригинални данни и псевдонимизирани такива се съхранява отделно от базата с данни, като към нея се предявяват завишени организационно технически мерки за сигурност – въвежда се функционалност на автоматизираните системи за запазване на съответствието, която е защитена с ниво на достъп само на определени служители и с технически средства за антивирусна защита;
3. достъпът до съответствието се ограничава (принцип "необходимост да се знае");
4. псевдоминимизираната база се интегрира в системата за сигурност на информацията на администратора;
5. псевдонимизираните данни се премахват в съответствие с разпоредбите на кодекса, когато целта за обработка вече е постигната.
(3) За ефективна псевдонимизация се прилагат следните правила:
1. всеки вид данни трябва да имат уникален псевдоним – имената може да се заменят в определени документи с клиентски номер;
2. за разбираемост псевдонимите съответстват на оригиналния формат и дължина на данните;
3. за някои данни (дата на раждане, ЕГН) стойностите могат да бъдат заменени с алтернативни (възраст, заместващ клиентски номер) или да са заменени от посочване единствено на клиетския номер;
4. формата на псевдонима трябва да показва, че не е "реална" информация;
5. псевдонимите за външна употреба са различни от псевдонимите за вътрешна употреба;
6. псевдонимната информация има същата сигурност както оригиналната.
(4) При предаване на данни на КЕВР за осъществяване контрол върху качеството на дейността на операторите или при друго предаване на данни, при възможност имената на потребителите се заменят с клиетски номера. Разкриването на връзката на номера с лични данни на потребителя се извършва при необходимост, законово задължение или правомерно искане на третото лице.

ГЛАВА ТРЕТА
ИНФОРМАЦИЯ И ПРАВА НА СУБЕКТИТЕ НА ЛИЧНИ ДАННИ
Раздел I.
Информиране на обществеността и на субектите на данни

Чл.33. (1) Настоящият кодекс се публикува по подходящ начин от наблюдаващия орган:

1. на интернет страницата на наблюдаващия орган;
2. на специално създадена информационна интернет страница за субекти, чийто данни се обработват от администратори, приели спазването на кодекса;
3. на интернет страницата на администратора, ако има такава.

(2) Екземпляр от кодекса се съхранява на хартиен или електронен носител от операторите, които прилагат кодекса.

Чл.34. (1) Наблюдаващият орган създава условия за информираност на субектите относно правата им по реда на Регламента и закона чрез създаването на специална информационна интернет страница.
(2) Наблюдаващият орган осигурява и възможности за отговор на конкретни запитвания чрез електронен адрес и форма за подаване на запитвания онлайн.

Чл.35. (1) Администраторите на лични данни предоставят на субектите данни относно идентификация на администратора и координати за връзка с него; координати за връзка с длъжностното лице по защита на данните; правото да бъде подадена жалба до наблюдаващия орган и до комисията и техните координати за връзка; информационната интернет страница на наблюдаващия орган и формата за подаване на сигнали, законово основание и преследваните цели, вида на обработваните лични данни и описание на правата на субектите в политика за конфиденциалност, която се поставя на видно място в помещенията на администратора.
(2) Информацията по ал.1 може да се предостави под формата на одобрени еднообразни брошури, разпространени в помещенията на операторите, които прилагат кодекса.
(3) Посочената информация се публикува и на интернет страницата на оператора, ако има създадена такава.
(4) Наблюдаващият орган обявява чрез интернет страницата всички администратори с техните данни за контакти, които са присъединени към спазване на кодекса.
(5) На видно място в помещенията на администратора или на интернет страницата му се поставя знак с лого на наблюдаващия орган и информация, че администраторът прилага настоящия кодекс.

Чл.36.(1) При поискване от субекта на данни при условия на чл.37, ал.4 се извършва изтриване, коригиране или ограничаване на данните в регистрите, за което субектите се уведомяват
(2) Трети лица – получатели на данни от регистрите, се уведомяват по предвидения в този кодекс начин за поправка или неточности в данните. В случаите, когато получателят на данните публичен субект (КЕВР, НАП, НОИ, органи на съдебната власт) определи, че е невъзможно да се актуализират вече предадени данни, администраторът не носи отговорност.

Раздел II.
Упражняване на правата на субектите на данни

Чл.37. (1) Правата на субектите на данни, определени в Регламента и в закона, са гарантирани от кодекса. Наблюдаващият орган и администраторите приемат мерки за навременно, пълно и ефективно приложение на правата на субектите.
(2) Правата на субектите се упражняват по следните начини :

1. предоставяне на информация по разбираем и навременен начин относно правата на субектите от администратора и определените от него длъжностни лица, натоварени с обработка на данните;
2. приемане на запитвания, заявления, възражения и жалби от администратора;
3. разглеждане на запитванията, заявленията, възраженията и жалбите в определените в закона и в Регламента срокове;
4. регистриране на подадените от субектите искания и други актове;
5. информиране на наблюдаващия и/или надзорния орган при необходимост.

(3) Субектите имат следните определени от Регламента права:

1. право на потвърждение и достъп до данните за субекта;
2. право на коригиране на данните;
3. право на изтриване на данните (право „да бъдеш забравен“);
4. право на ограничаване на обработването;
5. право на преносимост на данните;
6. право на възражение, включително относно решения при автоматизирано обработване на данните и профилиране;
7. право на обяснения при нарушения в режима на защита на данните;
8. право на жалба до наблюдаващия и до надзорния орган за нарушения на правилата за обработване на лични данни;
9. право на обезщетение и съдебна защита.

(4) Правата по ал.3, т.1 - 7 се упражняват с писмено заявление от субекта на данните или негов изрично упълномощен представител. Упълномощаването следва да бъде с нотариална заверка на подписите на субекта. При непълнолетни и лица с ограничена дееспособност, правата се упражняват със съдействието или чрез законните представители.
(5) Всяко лице, чийто данни се обработват има право да подава заявление относно данните, които се отнасят за него.
(6) Заявлението трябва да е в писмена форма и съдържа:
1. Име, единен граждански номер или клиентски номер, които са необходими за да може администратора да го идентифицира. Информация относно актуален адрес и данни за кореспонденция;
2. Предпочитаната форма, в която лицето иска да му се предоставя достъп до личните данни или да му се предостави отговор относно заявеното право;
3. Подпис, дата на подаване на заявлението.
(7) Правата не се разглеждат без заявление, попълнено по надлежния начин. Заявленията се подават по описаните в чл.37б, ал.2 и ал.3 от ЗЗЛД начини.

Чл.38. (1) Всяко заявление по чл.37, ал.4 се завежда в регистър, воден на хартиен или електронен носител.
(2) В регистър на заявленията се определят:
1. Графа № и дата – заявлението се завежда със съответния номер, в зависимост от поредността на неговото постъпване и датата. Всяка заявление се вписва с входящ номер;

2. Графа „име на заявителя” – посочва се кое лице подава заявлението или клиентския му номер;
3. Графа „изпълнение на искането” – посочва се датата на уведомяването и се удостоверява факта на връчване на съответния акт. В графата се вписва датата, на която лицето лично трябва да получи съответния акт.
4. Графа „отказ” – посочва се датата на неговото връчване и се удостоверява факта на самото връчване.
(3) Всяко заявление се подрежда в класьор или на електронен носител.
(4) Заявленията се съхраняват една година, след което се унищожават. Срокът за съхранение може да бъде удължен от администраторите, но не повече от 5 години.
(5) Достъп до заявленията имат администратора или определени от него длъжностни лица.
(6) Забранява се достъпа до заявленията от други лица, освен изброените в горната алинея.
(7) След като заявлението бъде разгледано, се уведомява субекта за предприетите действия или на коя дата да се яви, за да получи достъп до данните. При възможност правата се удовлетворяват дистанционно.
(8) Уведомлението се вписва и извежда в регистъра по описания по-горе начин.

Чл.39. (1) След завеждане на заявлението в регистъра се проверява неговота допустимост и законосъобразност съобразно Регламента и закона.
(2) Администраторът е длъжен да направи следното:
1. Да провери дали подаденото заявление отговаря на формалните законови изисквания.
2. Да провери дали подаденото заявление отговаря на материалните законови изисквания, дали лицето има основание и т.н.
(3) Посочените проверки се извършват от администратора в двадесетдневен срок от подаване на заявлението.
(4) Решението на администратора по подаденото заявление се издава в срок до 60 дни от датата на постъпване на заявлението.
(5) Решението се изпраща по посочените от субекта данни за контакт – писмо с обратна разписка, електронен адрес или факс, съответно отговор в потребителски интерфейс.
(6) Решенията, с които не се удовлетворява искането на субекта, съдържат правни и фактически основания за това.
(7) При заявленията по чл.37, ал.3, т.1-4, субектът на данните може да упражни правата си и чрез комисията (непряко упражняване на права). Администраторът информира субекта на данните за възможността да упражни правата си чрез комисията в решението.

Чл.40. (1) Субектът има право да посочи всяка една от формата на **достъп** до личните данни:
1. Устна справка;
2. Писмена справка;
3. Да прегледа лично документите си относно клиетската партида;
4. Копие от документите, в които се съдържат лични данни (освен, ако документът не е предоставен от самия субект на администратора);
5. Предаване на електронен път.
(2) Субектът, на който е разрешен достъп до личните му данни, няма свободен достъп до документите. Извлеченията на данните и копията от тях се правят от администратора на лични данни.

(3) Когато е необхфодими изнасяне на документи от помещенията за съхранение това се прави от администратора на лични данни, след вписване в регистъра на датата и причината за това. За длъжностното лице възниква задължението да върне документите след приключване на текущата работа не по - късно от края на работния ден.

Чл.41. (1) Достъпът до лични данни на недееспособно лице става след разрешение на законния представител на администратора.
(2) Администраторът преценява законосъобразността на поискания достъп и го разрешава и забранява.
(3) Документите съдържащи лични данни се предоставят лично или се изпращат в запечатан плик или папка по начин, който гарантира защитатат на личните данни в тях.

Чл.42. (1) Достъп до личните данни от регистрите имат всички държавни или обществени органи, които по силата на нормативен акт имат право на такъв достъп.
(2) Администраторът е длъжен да осигури поискания от държавните органи достъп да лични данни в регистъра без предварително писмено или устно разрешение от страна на техния титуляр.
(3) В случаите, когато по дела, водени от или срещу администратора, има назначена съдебна експертиза, достъп на съответното вещо лице се допуска само при представяне на изрично съдебно удостоверение, в което се посочва задачата на вещото лице и видът на носителите на информация, до които се иска достъп.
(4) Администраторът предоставя пълен или ограничен достъп до личните данни, като в случай на ограничаване на достъпа се посочват правните или фактически основания по закон за това.
(5) В случай, че администраторът установи, че няма право да предостави поисканата информация, се съставя решение за отказ, което съдържа правни и фактически основания : кои данни; поради каква причина и на какво основание се отказват за предоставяне; органът и срока, в който трябва да се обжалва частта на отказа - жалба до наблюдаващия орган, до комисията или търсене на защита по съдебен ред.

Чл.43. (1) Правото на **коригиране** на данните се основава на представени от субекта доказателства за неточностите – документи за вещни права, удостоверения, скици и схеми, декларации, удостоверения.
(2) В случаите, когато поправката се установява от публични регистри или се дължи на грешка в обработването от страна на администратора, не се изискват доказателства от субекта.
(3) Администраторът може да откаже коригиране на данните в регистрите по чл.7, ал.2когато за това е необходимо съдействие на публичен орган, на когато данните са предадени и това не е възможно или е необходимо специално административно или съдебно производство, което не е от компетентността на администратора.

Чл.44. (1) Субектът има право да иска **изтриване** на данните относно него на предвидените в Регламента и закона основания.
(2) Данните в регистрите не се изтриват, когато са обработени законосъобразно и е налице законово изискване за съхранението им до посочения срок на съхранение в закона или за нуждите на извършвани проверки от публични органи.

(3) В случаите по ал.2 субектът се уведомява, че данните му ще бъдат изтрити след изтичане на сроковете за съхранение на данни в съответния регистър, опрелени в кодекса.
(4) Данните се изтриват по предвидения в кодекса ред за унищожаване на носители на лични данни, като администраторът прави разумна проверка за всички материални и електронни носители на данни – досиета и папки, електронни записи, включително в автоматизирани системи за обработка на данни, електронна поща и други.

Чл.45. (1) Субектът има право на **ограничаване** на обработването на данните.
(2) Преди отмяна на ограничението администраторът уведомява субекта по предвидения в кодекса начин за уведомяване на решения по заявления.
(3) В случай, че субектът желае запазване на личните му данни след изтичане на определените в регистрите срокове за съхранение трябва да посочи и представи доказателства за причината за това – съдебни или административни производства и други. Администраторът определя разумен срок за ограничение на обработването предвид посочените от субекта причини.

Чл.46. Администраторът съобщава за всяко извършено коригиране, изтриване или ограничаване на обработване на всеки получател, на когото личните данни са били разкрити, освен ако това е невъзможно или изисква несъразмерно големи усилия – при предадени на КЕВР или друг орган данни в предварително определени форми, които не позволяват последващата корекция. Администраторът информира субекта на данните относно тези получатели, ако субектът на данните поиска това.

Чл.47. (1) Субектите имат право на **преносимост** на данните, ако те се обработват по автоматизиран начин и са структурирани във вид, който е широко ползван и пригоден за машинно четене.
(2) Преносимостта се извършва при ясно определяне в заявлението от страна на субекта кои данни ще бъдат обект на преносимост, точно идентифициране на получателя на данните и начина на предаване на данните, който да бъде съответен на организационните и технически мерки за защита на данните.
(3) Преносимостта се извършва, когато данните се обработнат по начин, позволяващ обособяване на данните на субекта от други данни, които не могат да бъдат пренесени.

Чл.48. (1) Субектите имат право на **възражения** при обработване на данните им.
(2) Субектите не могат да възразят срещу закономерното обработване на данни от регистрите при предоставени лично от субекта от документи за вещни права, удостоверения за наследници или други официални документи, попълнени декларации или удостоверения.

Чл.49. (1) В случаите на нарушение на сигурността на данните, за които субектът не е уведомен от администратора на основание чл.34, §3 от Регламента, субектът има право на **обяснение** от администратора.
(2) В предоставеното обяснение администраторът посочва вида на нарушението на данните, обхвата на данните, наличните технически и организационна мерки на защита, взетите мерки за ограничение на последиците от нарушението и препоръки към субекта.

Чл.50. (1) Субектите имат право на жалба до наблюдаващия кодекса орган.

(2) Жалбата се подава в писмена форма и отговаря на изискванията за подаване на заявления по кодекса.
(3) В жалбата се описват обстоятелствата относно нарушението на регламента, закона или кодекса и се прилагат доказателства за това.
(4) Наблюдаващият орган разглежда жалбата в срок от 60 дни, като изисква обяснения от администратора на личните данни.
(5) Субектите се уведомяват за взетото от наблюдаващия орган решение по жалбата и за евентуалните санкции за нарушение на кодекса спрямо администратора.
(6) Наблюдаващият орган има право да иска от субекта допълнителна информация и доказателства, с които субектът разполага.
(7) Жалбата до наблюдаващия орган не ограничава правото на жалба пред комисията и съдебната защита на правата на субектите.

Чл.51. (1) Субектите имат право на жалба пред комисията в случаи на обработване на лични данни в нарушение на регламента, закона или кодекса.
(2) Администраторът и наблюдаващия орган препращат в срок от 14 дни получени жалби на комисията, когато са получени от тях и са с адресат комисията. Администраторът има право да приложи становище по жалбата.
(3) Субектите имат право на обезщетения за нанесени вреди от нарушения при обработване на лични данни пред съда, компетентен по смисъла на чл.79, §2 от Регламента. Приложимото право за определяне на обезщетение за нанесени вреди се определя от Регламент 864/2007 относно приложимото право към извъндоговорните задължения.

Раздел III.
Информирането и закрилата на децата и начина за получаване на съгласие от носещите родителска отговорност за детето

Чл.52. (1) Обработването на лични данни на деца се извършва при получаване на изрично съгласие на законните им представители според приложимото към личния статут материално право, когато е необходимо съгласие. За български граждани законните представители се определят от Закона за лицата и семейството и Семеен кодекс – родители, настойници или попечители.
(2) Относно регистрите на потребителите на ВиК услуги не се изисква съгласие за обработване на данни, когато титуляр на правото на собственост или други вещни права е дете.
(3) При промоции и намаления, администраторът обяснява правата на децата на разбираем и прост език и не изисква събиране на данни извън имена на децата.
(4) В случай, че се налага обработване на лични данни на деца, информацията се предоставя на прост и разбираем език, като при възможност и според етапа на развитие на детето се предоставя в писмена форма.
(5) При обработване на лични данни на деца се обръща специално внимание на идентификацията на субектите. Ако лицата нямат издаден документ за самоличност, изисква се потвърждение от законен представител на детето.
(6) При обработка на лични данни на деца относно сключване на трудови договори от лица под 18 години администраторът предоставя информацията на субектите по ясен и

разбираем начин, включително изрично информира лицето относно всички права и задълженията на администратора, включително правото на детето да бъде забравено и другите права. Администраторът не събира данни, извън определените в трудовото и осигурителното законодателство и разяснява на детето, че основанието за обработване е законово задължение.
(7) При обработка на лични данни на деца относно ползване на отпуски от служители на администратора или с оглед ползване на право на обезщетения по реда на КСО, администраторът уведомява служителя относно правата на детето при обработка на данните и начина на упражняването им от страна на законния представител. Администраторът не събира данни, извън определените в трудовото и осигурителното законодателство и разяснява на родителя/детето, че основанието за обработване е законово задължение.
(8) При обработката на данни за деца за нуждите на маркетинговите дейности администраторите, присъединили се към този кодекс се задължават да използват най малко следните принципи:
1. политиките за прозрачност, ще бъдат формулирани по ясен и достъпен начин, разбираем за деца;
2. предлагането на онлайн услуги на деца е допустимо при планирано събиране на съгласие от родител или настойник;
3. прилагат се мерки за проверка на съгласието на родителя или настойника посредством подходящи технически решения (телефон, електронна поща и др.);
4. не се извършва профилиране на потребители под 16 години с никаква цел, включително анализ на техните интереси или предпочитания за маркетинг, без съгласието на родителите или настойниците;
5. всички искания за изтриване на данни за деца (фотографии или всяка друга информация, обработена въз основа на съгласието на детето) се приемат, независимо от възрастта на лицето в момента на искането им за изтриване на данните.
(9) При обработката на данни за деца като кандитати за работа администраторите, присъединили се към този кодекс се задължават да получат съгласие от носещият родителски права.

ГЛАВА ЧЕТВЪРТА
МЕРКИ И ПРОЦЕДУРИ ЗА СИГУРНОСТ И ОТЧЕТНОСТ НА ДАННИТЕ.

Раздел I.
Сигурност, анализ на риска и оценка на въздействието.

Чл.53.(1) Изграждането на цялостната система за защита на личните данни се постига чрез предварително извършен и документиран анализ на риска, евентуално и на оценка за въздействието.
(2) Постигането на подходящо ниво на сигурност е въз основа на анализ на конкретните рискове и оценка на въздействието.
(3) Анализът на риска се извършва преди започване обработването на данни във формат и обхват, одобрени от наблюдаващия орган.

(4) След оценка на въздействието, администраторите приемат една или повече от изброените минимални мерки на защита в кодекса, след прилагането на които се извършва нов анализ на риска.
(5) Ако въпреки предприетите мерки, влиянието на риска остава „значителен“ или „максимален“ за обработката на данните, длъжностното лице по защита на данните уведомява администратора, за необходимостта от консултация с надзорния орган.
(6) Анализ на риска се извършва най – малко в срок до 12 месеца след всяка предходна оценка.
(7) Администраторът поддържа запис на хартиен или електронен носител на направените в хронологичен ред анализи на риска, които да бъдат представени при поискване на наблюдаващия и на надзорния орган.

Чл.54. (1) Общият критерий за извършване на анализ на риска е осигуряване на адекватно ниво на защита на личните данни в поддържаните регистри с лични данни от рисковете, които са свързани с обработването, по-специално от случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или достъп до прехвърлени, съхранявани или обработени по друг начин лични данни. При анализа на риска се прилагат критерии за пропорционалност на обработването и съобразяване на подходящи мерки на защита спрямо вида на риска, вероятността за възникването му и тежестта на въздействието, които са необходими за защитата на данните.
(2) Методиката на анализ на риска се извършва в следните етапи :
1. анализ на рисковете по видове заплаха за данните и описание на нежеланите събития;
2. определяне на вероятността за възникване риска;
3. определяне на тежестта на въздействие на риска.
(3) След проверка на вероятността на реализиране на риска в съответствие с приетите технически и организационни мерки на защита, може да се направи анализ на остатъчната вероятност и ниво на въздействие. Анализът на риска е елемент от оценката на въздействието по този кодекс.

Чл.55. (1) От гледна точка на субекта на данните се определят възможни рискове за неприкосновеността на личния живот, които могат да бъдат в следните аспекти:
1. Неправомерно разкриване и достъп на лични данни;
2. Нарушена цялостност на лични данни;
3. Загуба (наличност) на лични данни;
4. Неправилна оценка или профилиране;
5. Невъзможност за упражняване на права съгласно законодателството за защита на данните.

(2) От гледна точка на вида на последиците на нежеланите събития, могат да се определят следните видове :
1. незаконосъобразен достъп до лични данни;
2. нарушение на цялостта на личните данни;
3. загуба на лични данни.
(3) Заплахите са събития или действия, съответно бездействия, които водят до реализиране на нежеланите последици. При оценката на риска се изброяват основните заплахи относно ползването на хардуер, софтуер, случайни събития и човешко поведение.
(4) Източниците на риск могат да бъдат :

1. вътрешни човешки източници - служители, ИТ мениджъри, стажанти, мениджъри;
2. външни човешки източници - получатели на лични данни (КЕВР, НАП, НОИ), упълномощени трети лица, доставчици на услуги, хакери, потребители и посетители, бивши служители, активисти, конкуренти, клиенти, персонал по поддръжка, поддръжка, нарушители, синдикати, журналисти, неправителствени организации, престъпни организации, организации под контрола на чужда държава, терористични организации, близко разположени промишлени дейности;
3. нечовешки източници - Зловреден код с неизвестен произход (вируси, червеи и т.н.), вода (тръбопроводи, водни пътища и т.н.), възпламеними, корозивни или избухливи материали, природни бедствия, епидемии, животни.

Чл.56.(1) Анализът на риска се извършва чрез ползване на матрици на рисковете, в която всеки един риск е определен чрез „вероятност за възникване“ и „тежест на въздействието“.
(2) Формите за анализ на риска съдържат следните минимални елементи :
1. вид риск;
2. основни източници на риска;
3. основни заплахи;
4. потенциални въздействия;
5. основни механизми за защита, намаляващи тежестта и вероятността;
6. тежест;
7. вероятност.
(3) Анализ се извършва за всички рискове, които могат да доведат до физическа, имуществена или неимуществена вреда на субекта на данните, включително всяка дискриминация, увреждане на репутацията, загуба на поверителност на данните, нарушаване на професионалната тайна, или други значителни икономически или социални неблагоприятни условия.
(4) В зависимост от анализа на риска се приема съответно ниво на мерки на защита, които са определени в този кодекс. Нивото на защита представлява съвкупност от технически и организационни мерки за физическа, персонална, документална защита и защита на автоматизираните информационни системи и/или мрежи, евентуално и криптографска защита на личните данни.

Чл.57.(1) Вероятността представлява възможността от възникването на даден риск. Тя се преценява преди всичко от гледна точка на нивото на уязвимост на съответните подпомагащи активи и нивото на възможностите на източниците на риск да ги използват, като се вземат предвид съществуващите, планираните или допълнителните системи за защита.
(2) Вероятността на възникване се определя чрез следните нива :
1. Пренебрежима: не изглежда възможно избраният източник на риск да материализира заплахата, като използва свойствата на подпомагащите активи (напр. кражба на хартиени документи, съхранявани в помещения на администратора, защитени с четец на баджове и код за достъп).
2. Ограничена: изглежда трудно избраните източници на риск да материализират заплахата, като използват свойствата на подпомагащите активи (напр. кражба на хартиени документи, съхранявани в помещение на администратора, защитена с четец на баджове и врати, които се заключват).

3. Значителна: изглежда възможно избраните източници на риск да материализират заплахата, като използват свойствата на подпомагащите активи (напр. кражба на хартиени документи, съхранявани в приемни помещения за работа с потребители на администратора, до които не е възможен достъп без персоналът да има визуален контрол).
4. Максимална: изглежда много лесно избраните източници на риск да материализират заплахата, като използват свойствата на подпомагащите активи (напр. кражба на хартиени документи, съхранявани в публично достъпната част на помещенията на администратора).

(3) Определеното ниво на вероятност може да бъде повишено или понижено чрез включване на допълнителни фактори:

1. отваряне на файлове в интернет или в затворена система;
2. обмени на данни с трети лица или не;
3. взаимовръзки с други системи или липса на взаимовръзка (електронни системи за предаване на данни за контрол на качеството на ВиК услугите);
4. хетерогенност или хомогенност на системата;
5. изменчивост или стабилност на системата;
6. репутация на оператора на ВиК услуги.

Чл.58. (1) Тежестта на въздействието на риска представлява величината на даден риск. Тя се оценява преди всичко от гледна точка на степента на потенциалните въздействия върху субектите на данни, като се вземат предвид съществуващите, планираните или допълнителните мерки за сигурност и контрол на обработването на данни.

(2) Тежестта на въздействие се определя чрез следните нива :

1. Пренебрежима - Субектите на данни или няма да бъдат засегнати или може да се изправят пред нови неудобства, които ще преодолеят без никакъв проблем
2. Ограничена - Субектите на данни могат да се изправят през значителни неудобства, които те може да са в състояние да преодолеят, макар и с известни затруднения;
3. Значителна - Субектите на данни може да се изправят пред значителни последици, които те следва да са в състояние да преодолеят, макар и с реални и сериозни затруднения;
4. Максимална - Субектите на данни може се изправят пред значителни или дори непоправими последици, които те не могат да преодолеят.

(3) Анализът на риска трябва да определи влиянието на риска.

(4) Влиянието на риска е произведение от тежестта и вероятността на риска.

Чл.59.(1) Оценка на въздействието се извършва от операторите на ВиК услуги с оглед на обхвата, контекста и целите на обработването, които могат да породят висок риск за правата и свободите на физическите лица. ВиК операторите обработват лични данни на всички лица, присъединени към водопреносната мрежа в дадена община, населено място или друга териториална единица, което предпоставя извършване на оценка на въздействието.

(2) Оценката на въздействието се основава на следните положения:

1.Основните принципи за обработка на данните и правата на субектите са непроменими и независещи от рисковете;

2. Неприкосновеността на субектите, свързана с техните лични данни, се постига с подходящи технически и организационни мерки за защита.

Чл.60. (1) Оценката на въздействието включва най-малко следните дейности:
1.системен опис на предвидените операции по обработване, цели на обработката и преследван законов интерес от ВиК операторите - описание на контекста на обработване на лични данни при предоставяне на ВиК услуги и оценка на необходимостта и пропорционалността на операциите по обработване по отношение на целите;
2.анализ на механизмите за контрол, гарантиращи спазване на основните принципи: пропорционалност и необходимост на обработването, и защитата на правата на субектите на данни;
3.оценка на рисковете за правата и свободите на субектите и гаранции, че рисковете от нарушение на неприкосновеността на личния живот са надлежно регулирани чрез подходящи мерки на защита;
4.текущо документиране на валидирането на оценката на въздействието с оглед на предхождащите факти, за да бъде предадена или да се преразгледат предходните стъпки.
(2) Когато е целесъобразно, администраторът се обръща към потребителите или към техни представители за становище относно планираното обработване, без да се засяга защитата на търговските или обществените интереси или сигурността на операциите по обработване.
(3) Лицата, които отговарят за дейностите по обработване на данни в регистрите по чл. 7, ал. 1, организират и участват в извършването на оценката на въздействието под ръководството и наблюдението на длъжностното лице по защита на данните.
(4) Когато обработването е с основание в националното или европейско право и това право регулира конкретната операция по обработване или набор от такива операции, и вече е извършена оценка на въздействието върху защитата на личните данни като част от общата оценка на въздействието в контекста на приемането на това правно основание, не се извършва анализ на въздействието.

Чл.61. (1) Оценката на въздействието е постоянен процес, който налага текущо наблюдение на промените в елементите по чл.60, ал.1 и се актуализира най - малко веднъж годишно. При възникване на значителни промени се извършва извънредна актуализация на оценката. Прегледът се извършва когато има промяна в риска, с който са свързани операциите по обработване.
(2) Преглед се извършва при планирано обработване на нов вид данни.
(3) При резултат от извършената оценка, че обработването ще породи висок риск въпреки предприетите от администратора мерки за ограничаване на риска, администраторът се консултира с наблюдаващия орган, който му дава задължителни предписания. Ако обработването не е започнало и/или се отнася за нов регистър, администраторът може да се обърне за консултация и към Комисията.

Чл.62.(1) Първият етап на оценката на въздействието включва оценка на контекста на обработването на данните.
(2) Администраторът следва да документира :
1. кратко описание на обработването – описание (обхват), цели, интереси, идентифициране на определените обработващи данните лица и предаване на данните на трети лица;
2. посочване на източници на уредба на обработването – специални нормативни актове (ЗРВКУ, Наредба № 4 от 14.09.2004г. за условията и реда за присъединяване на потребителите и за ползване на водоснабдителните и канализационни системи, Наредба за регулиране на качеството на водоснабдителните и канализационни услуги, Указания на

КЕВР, одобрени общи условия на ВиК операторите; общи – Регламента, ЗЗЛД, указания и актове на Комисията, настоящия кодекс)
3. данни и процеси по обработване – видове лични данни, техните получатели и сроковете за съхранение; описание на процесите за целия цикъл на работа с данните (от събирането при първоначално заявление за присъединяване към водопреносната система или заявяване на друга услуга до унищожаване на данните) и по – специално относно потребилите на ВиК услуги.

Чл.63. (1) Вторият етап на извършване на оценката на въздействието е относно оценката на мерките за контрол, гарантиращи необходимостта и пропорционалността на обработването.
(2) Администраторът следва да удостовери, че обработването отговаря на следното:
1.ясно определени цели за всеки регистър: конкретни, изрично указани и легитимни;
2.основание на обработването за всеки регистър : законосъобразност на обработването (изпълнение на договор, законови задължения, легитимни интереси и т.н.), забрана за злоупотреби;
3.свеждане на данните до минимум: данните да бъдат подходящи, свързани и ограничени;
4.проверка на качеството на данните: точни и поддържани актуални данни.
5.срокове на съхранение: да бъдат ограничени по обективни критерии (общи данни, архивирани данни, функционални следи).
(3) За всеки от посочените в ал.2 показатели се прави проверка за възможно подобрение или за липса на необходимост, съответно възможност за това.
(4) При необходимост се предвиждат допълнителни мерки за контрол на обработването.
(5) Прави се оценка на процедурите, гарантиращи правата на субектите на данни, относно:
- информираност на субектите на данни (добросъвестно и прозрачно обработване);
- необходимост от съгласие – само при определени дейности по обработване – възможност да бъде доказано и оттеглено;
- право на достъп и право на преносимост на данните на потребителите;
- право на ограничаване на обработването и право на възражение;
- обработващи данни – установени и обвързани от договор;
- предаване на данни извън ЕС.

Чл.64.(1) Третият етап на оценката на въздействието се извършва относно оценка на рисковете за сигурността на данните съгласно определените по – горе методи и показатели на оценката на риска.
(2) Извършва се проверка относно съответствието на предприетите мерки за защита с вида на рисковете и дали се прилагат най-добрите мерки за сигурност, освен ако не е необходимо или не е възможно това.
(3) Проверява се съдържанието на въведените мерки за защита срещу рисковете и се предлагат нови, ако е необходимо.

Чл.65. (1) Четвъртият етап на оценката на въздействието се състои в заключителен акт на оценката, наречен валидиране.
(2) Валидирането се подписва от законния представител на администратора или от определено от него длъжностно лице.
(3) Констациите от извършената оценка се обобщават :
- презентация на мерките за контрол, избрани, за да се осигури спазване на основните

принципи за обработка на лични данни;
- презентация на мерки, насочени към осигуряване на сигурността на данните;
- карта на рисковете при дейността на ВиК операторите (първоначални и остатъчни) според вероятността и тежестта им;
- план за действие въз основа на допълнителните мерки за контрол, установени по време на предишните стъпки: за всяка мярка на контрол се определя отговорно за изпълнението лице, цена на мярката (финансова или от гледна точка на работната натовареност) и прогнозен срок за внедряване.
(4) Вземат се предвид препоръките на длъжностното лице по защита на данните и на субектите на данни, ако имат отправени такива.
(5) Крайният акт на оценката на въздействието може да бъде валидирана, приемане под условие за подобрения или отрицателна (обработването следва да се преустанови).
(6) За да бъде издадена валидирана оценка е необходимо да се прецени дали въведените мерки за контрол, остатъчни рискове и план за действие са подходящи предвид интересите и правата на субектите на данните.
(7) При необходимост част от процеса на оценката на въздействието се повтаря за изграждане на крайната оценка на мерките.

Раздел II.
Технически и организационни мерки за защита на данните

Чл.66. (1) Администраторите въвеждат технически и организационни мерки в съответствие с извършен анализ на риска и оценка на въздействието и резултатите от тях.
(2) Предприетите мерки са в следните области:
1. физическа защита;
2. персонална защита;
3. документална;
4. защита на автоматизирани системи и мрежи
5. Криптографска защита.

Чл.67. (1) Приетите мерки се проверяват текущо и се изпитват чрез следните действия :
1. извършване на проверки за спазване на мерките на физическа, документална, персонална, автоматизирана защита най – малко веднъж на 12 месеца за резултатите от които се попълва одитен лист с означение на датата на проверката и попълнилия листа;
2. проверка на изправността на техническите устройства за автоматизирано обработване на данни от специализирани доставчици на услуги по поддръжка на техниката;
3. проверка на знанията на персонала чрез провеждане на обучения и подходящо форма на изпит;
4. изготвяне на препоръки за промени или въвеждане на нови подходящи мерки на защита при валидиране на оценката на въздействието;
5. анализ на получени жалби и искания за упражняване на правата от субекти на данните;
6. изпълнение на препоръки на наблюдаващия орган за повишаване на нивото на защита на данните.
(2) Според тежестта на въздействие при анализа на риска се осигуряват следните технически и организационни мерки за защита на данните :

1. При пренебрежима тежест – мерки за физическа защита по чл. 68, ал.1, т.2,3,6,7, 9 и 11, мерки за персонална защита по чл.69, ал.1, т.1,2,3,7 - 10, мерки за защита на автоматизирани системи по чл.71, ал.1, т. 1-3, 6 и 8 и ал.2, мерки за документална защита по чл.70, т.1-4, мерки за криптографска защита по чл.72, ал.1, т.1 и 6;
2. при ограничена тежест – посочените в т.1 мерки и в допълнение - мерки за физическа защита по чл. 68, ал.1, т.1,5 и 8, мерки за персонална защита по чл.69, ал.1, т.4, мерки за защита на автоматизирани системи по чл.71, ал.1, т.4 и 5, мерки за документална защита по чл.70, т.1-4;
3. при значителна тежест – посочените в т.2 мерки и в допълнение - мерки за физическа защита по чл. 68, ал.1, т.4, мерки за персонална защита по чл.69, ал.1, т.5, мерки за защита на автоматизирани системи по чл.71, ал.1, т.8-12 и ал.3 и ал.4, мерки за документална защита по чл.70, т.1-4, мерки за криптографска защита по чл.72, ал.1, т.2-4, 6-7;
4. при максимална тежест – всички мерки по чл.68 – 72.

Чл.68. (1) Администраторът приема в комбинация някои или всички от следните мерки за **физическа защита:**

1. Определяне на зони за контролиран достъп за обработка и съхранение на данни и ясно обособяване на зони за работа с потребители (фронт офиси), режим на движение във фронт офисите и контрол на достъпа до зоните със съхранение на данни. Поддържане на актуален списък на лицата (включително посетители, служители, овластени служители, обучавани лица и доставчици на услуги), които са овластени да влизат във всяка зона;
2. Заключване на помещенията, в които се съхраняват лични данни;
3. Предпазни решетки или ролетни щори на врати и прозорци;
4. В приемните помещения достъпът през работното време се контролира от служители на администратора или охранители. Въвеждат се методи за удостоверяване на идентичността на посетителите (например, лица, които идват, за да присъстват на среща, външни доставчици на услуги или потребители), съразмерни на рисковете, свързани с всяка зона;
5. В извънработното време достъпът се контролира чрез сигнално охранителна система или сключен договор за охрана с лицензиран по закон изпълнител;
6. Помещенията, в които се обработват лични данни са оборудвани с заключващи се врати, затворени или заключващи се шкафове и/или каси, пожарогасителни средства.
7. Всички изисквания на противопожарната и аварийна безопасност съгласно действащото законодателство се спазват, като в помещенията се поддържат изправни пожарогасители и други противопожарни системи.
8. Въвежда се самостоятелен код на сигнално – охранителните системи за достъп до помещенията на отделните служители. Монтират се заключващи се врати с цифров код или видеофон; редовно се обновяват начините за достъп (кодовете за отваряне на врати); обозначават се зони със забранен достъп на външни лица с ясни, видими знаци, които могат да бъдат разбрани от всички посетители;
9. Лица, извън оторизирания персонал, нямат достъп до ключовете за помещенията и шкафовете или други защитени пространства;
10. При възможност се въвежда система за достъп с отваряне с персонални магнитни карти и определяне на достъпа на съответни нива според длъжността;

11.Опасни продукти (включително възпламеними, запалими, корозивни, експлозивни, аерозолни и мокри вещи) се съхраняват в подходящи зони за съхранение и на безопасно разстояние от зоните, в които се обработват лични данни.

(2) Мерките на допълнителна физическа защите се описват в Процедури за обработка на данните, които се представят на наблюдаващия орган и съдържат правила за визуален достъп до документи, съдържащи лични данни; място и време на обработката; правила за изпращане на данни по отдалечен път и т.н.

Чл.69. (1) Администраторът приема в комбинация някои или всички от следните мерки за **персонална защита:**

1. достъпът до лични данни се осъществява само от лица, чиито служебни задължения или конкретно възложена задача налагат такъв достъп, при спазване на принципа „Необходимост да знае“. Лицата, които обслужват потребители, се легитимират с баджове, съдържащи име и длъжност;

2. всички служители са длъжни да спазват ограниченията за достъп до личните данни, и са персонално отговорни пред законния представител на администратора за нарушаването на принципите за обработка на личните данни.

3. лицата, обработващи лични данни при постъпване на работа се запознават с:

-нормативната уредба в областта на защита на личните данни и актовете по нейното прилагане, а именно: Регламента, Закон за защита на личните данни и подзаконови актове по прилагането му, кодекса и указания на Комисията;

- рисковете за личните данни, обработвани от администратора;

- ползване на образци на документи.

4. най-малко веднъж годишно се провежда обучение, в която програма е включено запознаване с кодекса, както и с актовете по т.3.

5. най-малко веднъж годишно се провежда тренировка на персонала за реакция при събития, застрашаващи сигурността на данните.

6. лицата, обработващи лични данни, задължително подписват декларация, неразделна част от съдържанието на трудовото или гражданско правоотношение, с която поемат задължение за неразпространение на лични данни станали им известни във връзка и по реме на изпълнение на служебните им задължения. Декларацията се съхранява в кадровото досие на всеки служител.

7. споделяне на лични данни между служителите (като идентификатори, пароли за достъп и т.н.) е забранено, освен с оглед обективното разпределение на трудовите функции.

8. обработване на лични данни се извършва само в работно време в помещенията на администратора на лични данни;

9.назначават се служители, които са добре квалифицирани за работата си. Ако нямат подходяща квалификация, администраторът осигурява обучение.

10. администраторът осигурява условия на труд на лицата с достъп до лични данни и обработващи лични данни, които са задоволителни.

(2) Периодичните обучения и тренировки по ал.1, т.4 и т.5, както и декларацията по ал.1, т.6, се документират чрез образци, представени на наблюдаващия орган.

(3) Администраторът приема правила за поведение на персонала относно съхранение на данните, които са част от друг акт или са самостоятелни.

Чл.70.Администраторът приема в комбинация някои или всички от следните мерки за **документална защита:**
1. Всички документи на хартиен носител, съдържащи лични данни (документи за вещни права, удостоверения за наследници, декларации, заявки, молби и др.), се съхраняват в заключени шкафове в помещения с ограничен достъп само за упълномощени лица, съответно в затворени шкафове в зоните на офисите, в които външни лица нямат пряк достъп;
2. личните данни могат да бъдат размножавани и разпространявани от упълномощените служители само ако е необходимо за изпълнение на служебни задължения или ако са изискани по надлежния ред от оправомощени лица;
3. забранено е изнасяне от помещенията на администратора на носители на данни, изпращането им по електронен път или копиране на електронни носители извън непосредственото изпълнение на законовите изисквания за предаване на данни;
4. забранен е предоставяне на достъп до данни на трети лица, както и унищожаването на данни, за които срокът на съхранение не е изтекъл или няма законосъобразно нареждане от адмистратора или от субекта на данните.

Чл.71. (1) Администраторът приема в комбинация някои или всички от следните мерки за **защита на автоматизирани системи и електронни носители и обмен на данни:**
1. автоматизирана обработка на данни се извършва с помощта на специализирани приложни софтуерни продукти и чрез стандартни средства за текстообработка, електронни таблици и др. (офис-пакети);
2. при електронната обработка се използват само лицензирани системни и приложни софтуерни продукти;
3. упълномощените служители за работа с данните задължително трябва да притежават необходимата компютърна грамотност и умение за работа с използваните специализирани софтуерни продукти;
4. всеки упълномощен потребител на автоматизирани системи и машини има личен профил с определени нива на достъп, съобразни със неговите задължения и принципа „Необходимост да знае“;
5. идентификацията и автентификацията на потребителите се реализира със средствата на операционната система и на използваните специализирани софтуерни продукти чрез потребителско име и парола;
6. заличаването на личните данните в електронен вид се осъществява чрез стандартните средства на операционната система или със средствата на специализираните софтуерни продукти;
7. в помещенията, в които са разположени компютърни и комуникационни средства, е осигурено заключване на помещенията, система за ограничаване на достъпа, сигнално-охранителна система;
8. работните компютърни конфигурации, както и цялата IT инфраструктура, включително и достъпът до интернет, се използват единствено за служебни цели;
9. забранено е използването на преносими носители на данни за лични нужди;
10. не се разрешава осъществяването на отдалечен достъп до данни от регистрите, освен при съхранение на данни на облачни сървъри, които прилагат ISO 27000 : 2017 и се намират на територията на ЕС;

11. за защита на данните е инсталирана антивирусна програма и се извършва седмична профилактика на софтуера и системните файлове;
12. администраторът на автоматизираните системи създава и поддържа базови конфигурации за защита на операционната система, защитни стени, рутери и мрежови устройства. Същият следи за своевременно обновяване (update) на системния, технологичния (офис-пакети и др.), приложния и антивирусния софтуер;
(2) В системите за автоматизирано обработване се водят записи (логове) най-малко за следните операции по обработване: събиране, промяна, справки, разкриване, включително предаване, комбиниране и изтриване, като системите имат функции по подходящо периодично архивиране на данните (бек - ъп) и съхранение на резервни копия.
(3) Записите за извършена справка или разкриване трябва да дават възможност за установяване на основанието, датата и часа на такива операции и доколкото е възможно — идентификацията на лицето, което е направило справка или е разкрило лични данни, както и данни, идентифициращи получателите на тези лични данни.
(4) Предаването на данни по отдалечен електронен път се извършва само в криптирана връзка, като не се предават лични данни с обикновена лична електронна поща на служителите.
(5) Администраторът документира мерките за защита на автоматизирани системи и електронни носители и обмен на данни със следните документи :
1. Опис на техническите средства – компютърни конфигурации и други устройства за приложение на автоматизираните системи;
2. Одитен лист за проверка на спазването на изискванията от персонала;
3. Процедури за достъп, контрол и смяна на пароли за достъп до автоматизирани системи и електронни носители на данни.

Чл.72. (1) Администраторът приема в комбинация някои или всички от следните мерки за **криптографска защита:**

1. използване на стандартните криптографски възможности на операционната система, на системите за управление на бази данни, на комуникационното оборудване, както и квалифицирани електронни подписи (КЕП);
2. изграждане на решения за сигурност, включващи криптиране на мрежовия трафик и защита от зловредни атаки на работната станция;
3. решения за мрежова защита от зловреден код; внедряване на централизирано антивирусно решение; филтриране на уеб трафика; антиспам защита (защита от нежелани електронни съобщения); защита от непознати интернет атаки;
4. изграждане сигурно хранилище, достъпно посредством криптирана връзка;
5. въвеждане на решения за псевдонимизиране на данните;
6. определя се обхвата на криптиране на данните (включително цял твърд диск, дял, хранилище, определени файлове, данни от база данни или комуникационен канал и т.н.) въз основа на формата, в която се съхраняват данните, установените рискове и изискуемото изпълнение;
7. избира се вид на криптирането (симетрично или асиметрично) въз основа на контекста и идентифицираните рискове.

(2) Администраторът въвежда организация за архивиране на данни на електронни носители, която осигурява запазване и управление на електронните архиви, съдържащи личните данни, за да се гарантира тяхната устойчивост през целия необходим период (прехвърляне,

съхранение, мигриране, достъпност, отстраняване, политика за архивиране, защита на поверителност и т.н.).
(3) При архивиране на данните се прилагат методи за достъп, които са специфични за архивираните данни, архивите се криптират и ползват нови ключове преди края на жизнения цикъл на криптиращите ключове, редовно се заменят остарели хардуерни активи за данни; избира се процедура, гарантираща, че целият архив е бил унищожен при заличаване на данните.

Чл.73. (1) При възникване и установяване на инцидент (природни бедствия, престъпни посегателства от трети лица) веднага се докладва на законния представител на администратора и в зависимост от обстоятелства, се уведомяват съответните институции. От компетентните органи се изисква включване в съответните протоколи и актове на бележка относно загуба или повреждане на носители на лични данни.
(2) С наличните ресурси се вземат мерки за ограничаване въздействието върху регистрите, ако това е възможно. Всички мерки за ограничаване на последствията от инцидента (възстановяване на документи и други) не трябва да водят до допълнителни рискове за обработката на данните и се съгласуват с длъжносното лице по защита на данните, ако е назначено такова.
(3) За инцидентите се води дневник, в който задължително се вписват предполагаемото време или период на възникване, времето на установяване, времето на докладване и името на служителя, извършил доклада. След анализ на инцидента, в дневника се описват последствията от инцидента и мерките, които са предприети за отстраняването им.
(4) В случаите на необходимост от възстановяване на данни, процедурата се изпълнява след писменото разрешение на законния представител на администратора, като това се отразява в дневника по архивиране и възстановяване на данни.
(5) За инцидентите се уведомява наблюдаващия орган и длъжностното лице по защита на данните. В случаи на нарушения на сигурността на личните данни се прилагат правилата на кодекса за уведомление на надзорния орган.
(6) Администраторът изпълнява предписанията на наблюдаващия орган, които са задължителни.
(7) Адмистраторът взема предварителни мерки за възстановяване на данните чрез :
1. съхранение на преписи от документи в електронен вид, когато е възможно;
2. въвеждане на настройки за периодично архивиране (бек ъп) на данните в автоматизирани системи за обработка;
3. регулярно архивиране на данни, които не се пряко необходими за изпълнение на дейността на администратора в нарочни помещения, които отговарят на изискванията за физическа защита по този кодекс.

Чл.74. (1) Всяко унищожаване на данни е контролирано и се извършва след изтичане на определените срокове за съхранение в съответните регистри и при спазване на изискванията за предаване на данни на Национален архивен фонд или на други публични органи.
(2) За унищожаване на лични данни администраторът назначава комисия.
(3) Документите, съдържащи лични данни, се унищожават по начин, непозволяващ тяхното възстановяване, например чрез нарязване на специално устройство (шредер) или изгаряне.
(4) След унищожаването на документите комисията съставя протокол и го представя на администратора и на длъжностното лице по защита на данните.

(5) Предаването на трети лица на носители за унищожаване на документи или други носители на данни се извършва след поемане на задължения за спазване на изискванията на кодекса от третото лице.
(6) Данните на електронен носител се унищожават чрез съответните команди и проверка за наличие на временни или други копия в операционната система, както и на копия на външни носители – външни дискове, дискове, флаш памет и т.н.
(7) При унищожаване на данните се прави проверка в служебната електронна поща за изпратени по електронен път преписи и съобщенията се изтриват, като се изпраща съобщение до получателя да извърши същата операция.

Чл. 75 (1) Администраторът осъществява следните минимални мерки за постоянна поверителност на данните : мерки за физическа защита по чл. 68, ал.1, т.1,2,3,4,6 и 9 , мерки за персонална защита по чл.69, ал.1, т.1, 7 и 8 - 10, мерки за защита на автоматизирани системи по чл.71, ал.1, т.4, 5, 7 и 9, мерки за документална защита по чл.70, т.1-4, мерки за криптографска защита по чл.72, ал.1, т.1, 3, 6-7 и ал.3, както мерките по чл.73, ал.2 при нежелано събитие и правилата за унищожаване на данни по чл.74. В допълнение, при всяко предоставяне на хардуерни или други носители на данни за ремонт или друга услуга на трети лица се подписват споразумения за конфиденциалност.
(2) Администраторът осъществява следните минимални мерки за наличност на данните : мерки за физическа защита по чл. 68, ал.1, т.4, 8 и 11, мерки за персонална защита по чл.69, ал.1, т.3 и 4, мерки за защита на автоматизирани системи по чл.71, ал.1, т.1, 2, 3, 11 и 12 и ал.2 и ал.3, мерки за документална защита по чл.70, т.2 и 4, мерки за криптографска защита по чл.72, ал.1, т.2-4, т. 6-7, ал.2 и ал.3. В допълнение, администраторът осигурява условия за минимално съхранение на лични данни на преносими устройства, като информация се прехвърля текущо на стационални устройства. При извършване на криптиране и архивиране се водят записи на местоположението на данните и на ключовете за достъп. Осигуряват се правила за наличност на кодове за достъп до автоматизираните системи и програмни кодове при временна загуба или срив на системите.
(3) Администраторът осъществява следните минимални мерки за цялостност на данните : мерки за физическа защита по чл. 68, ал.1, т.4-6, 8, 9 и 11, мерки за персонална защита по чл.69, ал.1, т.2,4,6 и 8 - 10, мерки за защита на автоматизирани системи по чл.71, ал.1, т.2- 8 и 11, мерки за документална защита по чл.70, т.3 и 4, мерки за криптографска защита по чл.72, ал.1 т.2, 3 и 7, както и мерките по чл.73, ал.4. Също така, администраторът създава организация за предупреждение в случай на нежелано изменение или изчезване на лични данни (хаш функция, код за удостоверяване на съобщения, електронен подпис, предотвратяващ внедрявания на SQL код и т.н.).
(4) Администраторът осъществява следните минимални мерки за устойчивост на данните : мерки за физическа защита по чл. 68, ал.1, т.7, мерки за персонална защита по чл.69, ал.1, т.4 и 5, мерки за защита на автоматизирани системи по чл.71, ал.1, т.1, 2,3, 6, 11 и 12 и ал.2 и ал.5, мерки за криптографска защита по чл.72, ал.1, т.2, 3, 6-7 и ал.2, както и мерките по чл.73, ал.7.

Чл.76. (1) При изпълнение на изискванията на Регламента и на закона, администраторът определя длъжностно лице по защита на данните.

(2) Администраторът обявява на видно място в помещенията си данни за контакт с длъжностното лице по защита на данните и на интернет страницата си, ако поддържа такава.
(3) Администраторът уведомява наблюдаващия орган за координатите на длъжностното лице по защита на данните.
(4) В допълнение на определените в Регламента и в закона задължения, длъжностното лице по защита на данните:
1. познава и следи за прилагане на кодекса при извършване на дейността на администратора;
2. обучава персонала на администратора и проверява спазването на изискванията на кодекса;
3. осъществява контакти с наблюдаващия орган и спазва неговите предписания относно приложението на кодекса;
4. съобщава на администратора за пропуски в режима на защита на личните данни и при непридприемане на мерки от страна на администратора, уведомява наблюдаващия орган;
5. съдейства на администратора за прилагане на кодекса и на образците на документи, одобрени от наблюдаващия орган за прилагането му.
(5) Администраторите са длъжни да провеждат най – малко веднъж годишно обучение на длъжностните лица за защита на данните и да осигурят необходимите условия за изпълнение на задълженията им от организационен, персонален или финансов характер.
(6) Администраторите оценяват всички препоръки и доклади на длъжностните лица за защита на данните и съобразяват дейността си с тях.

Чл.77. (1) Администраторът възлага на всички обработващи данни задължения относно спазването на настоящия кодекс чрез нарочни договори. В договорите се уреждат още предмета и срока на обработването, естеството и целта на обработването, вида лични данни и категориите субекти на данни, задълженията и правата на администратора.
(2) При съгласие от администратора обработващия данни да прибави друг обработващ, този друг обработващ приема задължения за спазване на изискванията на кодекса.
(3) Обработващият данни приема с договора да спазва предписанията на наблюдаващия орган и да му предоставя необходимото съдействие за контрол относно спазването на кодекса.

Раздел III.
Уведомяването на надзорните органи за нарушения на сигурността на личните данни и съобщаването за такива нарушения на сигурността на личните данни на субектите на данни

Чл.78. (1) Всички лица от персонала на администратора, длъжностните лица по защита на данните и обработващите данни докладват всяко съмнително събитие или инцидент на законния представител на администратора.
(2) Администраторът разследва възможно най-бързо и в срок не по-дълъг от два работни дни всеки доклад за инцидент. При разследването се включват длъжностното лице по защита на данните и лице, натоварено със защита на данните в структурата на администратора.

Чл.79. Следните мерки и действия се вземат при инциденти:

1. При кражба на носители на лични данни или достъп на неоправомощени лица до зона с достъп до лични данни:

- Проверка на Опис на техническите средства за обработка на данните, за да се установи кое средство липсва;
- Проверка на основанието за липса на носител на информация – преместване в друго помещение, поправка и др.
- При неправомерно отнемане на носителя, уведомяване на органите на МВР в рамките на същия ден с изрично указване на вида и обхвата на личните данни, които се съдържат на носителя;
- Оценка на необходимостта от допълнителни мерки на защита – промяна на пароли за достъп, смяна на ключалки на помещения и шкафове и др.

2. При осъществен достъп извън персонала на администратора до регистрите с данни:

- Събиране на данни от персонала на администратора в рамките на същия ден;
- Проверка от доставчици на интернет и поддръжка на автоманични средства за обработка на данните, включително одит на системата;
- Обяснения от субектите на данни;
- Оценка на необходимостта от допълнителни мерки на защита – промяна на пароли за достъп, смяна на ключалки на помещения и шкафове и др.

3. При неправилно унищожаване и изхвърляне на публични места на носители на данни:

- Проверка как носителите са попаднали на публични места;
- Предприемане на мерки за предотвратяване на нови инциденти – дисциплинарни наказания, обучения и консултации на персонала.

4. При жалби от клиенти, членове на персонала, контрагенти или други субекти на данни за нарушения на изискванията за защита на данните :

- Снемане на обяснения и информация от жалбоподателя;
- Разследване на обстоятелствата по подходящ начин и предприемане на пропорционални допълнителни мерки за възстановяване на данните и защитата им;
- Оценяване на нарушението според критериите за регистриране и уведомяване на надзорните органи.

5. Загуба на данни при изпращане на трети лица (КЕВР, НОИ, НАП и др.):

- Проверка на начина на изпращане на данните – електронно криптирано чрез подпис с КЕП; в затворен плик и т.н.;
- Анализ на възможните пропуски – предаване на КЕП на неоправомощетно лице, незапечатване на пощенски плик, ползване на прозрачен плик и т.н.;
- Уведомяване на получателя на данните (НАП, НОИ и др.) за възможни пробиви в сигурността на системата му за обработка на данни

Чл.80. (1) Всяко нежелано събитие, съдържащо опасност или нарушение на сигурността на данните се вписва в нарочен регистър на инциденти. В регистъра се описват фактите, свързани с нарушението на сигурността на личните данни, последиците от него и предприетите действия за справяне с него според одобрен от наблюдаващия орган образец на доклад за нарушение.

(2) Събитията се квалифицират в пет категории според тежестта им – пренебрежим риск (няма данни за достъп на трети лица до данните; данните не са напускали контролирана среда и не са предавани отдалечено; засегнати са по – малко от три лица), ограничен риск (данните са изгубени или има достъп на трети лица, но са защитени надлежно с криптиране и по друг начин, непозволяващ четенето им от третите лица; засегнати са до двадесет лица), значителен (данните не са защитени за четене и възпроизвеждане; данните се отнасят до 1000 лица; данните са специална категория) и максимален риск (цялостен достъп до данните от даден регистър; засегнати над 1000 лица). При преценката на риска се взема предвид – дали данните са загубени или унищожени в контролирана среда (помещенията на администратора); загуба на носители на информация на публично място; достъп на неоправомощено лице до данни. При категориите значителен и максимален риск е необходимо да бъде изпратено уведомление до Комисията, както и да се уведомят субектите на данни.
(3) Длъжностното лице по защита на данните или администраторът оценяват вида на риска и последващите изисквания за уведомяване на наблюдаващия орган, Комисията, засегнатите субекти, органите на МВР, НАП и застрахователни дружества.

Чл.81. (1) В случай на нарушение на сигурността на личните данни администраторът, без излишно забавяне, но не по-късно от 72 часа след като е разбрал за него, уведомява Комисията за нарушението на сигурността на личните данни, освен ако няма вероятност нарушението на сигурността на личните данни да доведе до риск за правата и свободите на физическите лица (пренебрежим или ограничен). Когато уведомлението до Комисията не е подадено в срок от 72 часа, то се придружава от причините за забавянето.
(2) Обработващият лични данни уведомява администратора без излишно забавяне, след като е установил нарушение на сигурността на лични данни.
(3) В уведомлението до Комисията се съдържа следното:
1. описание на естеството на нарушението на сигурността на личните данни, включително, когато това е възможно, категориите и приблизителния брой на засегнатите субекти на данни и категориите и приблизителния брой на засегнатите записи на лични данни;
2. посочване на името и координатите за връзка на длъжностното лице по защита на данните или на друга точка за контакт, от която може да се получи повече информация;
3. описание на евентуалните последици от нарушението на сигурността на личните данни;
4. описание на предприетите или предложените от администратора мерки за справяне с нарушението на сигурността на личните данни, включително по целесъобразност мерки за намаляване на евентуалните неблагоприятни последици.
(4) Когато и доколкото не е възможно информацията да се подаде едновременно, информацията може да се подаде поетапно без по-нататъшно ненужно забавяне.
(5) Препис от уведомлението се изпраща и на наблюдаващия орган.

Чл.82. (1) Когато има вероятност нарушението на сигурността на личните данни да доведе до ограничен, значителен или максимален риск за правата и свободите на физическите лица, администраторът без излишно забавяне съобщава на субекта на данните за нарушението на сигурността на личните данни.
(2) В съобщението до субекта на данните, на ясен и прост език се описва естеството на нарушението на сигурността на личните данни и се съдържат най-малко информацията и мерките, посочени в чл. 81, ал. 3, точки 2, 3 и 4.

(3) Посоченото в ал. 1 съобщение до субекта на данните не се изисква, ако е изпълнено някое от следните условия:
1. администраторът е предприел подходящи технически и организационни мерки за защита и тези мерки са били приложени по отношение на личните данни, засегнати от нарушението на сигурността на личните данни, по-специално мерки, които правят личните данни неразбираеми за всяко лице, което няма право на достъп до тях, като например криптиране или анонимиризиране;
2. администраторът е взел впоследствие мерки, които гарантират, че вече няма вероятност да се материализира високият риск за правата и свободите на субектите на данни;
3. то би довело до непропорционални усилия. В такъв случай се прави публично съобщение или се взема друга подобна мярка, така че субектите на данни да бъдат в еднаква степен ефективно информирани. Публичното съобщение се изпраща и до наблюдаващия орган за публикуване на специално създадена информационна интернет.
(4) Съобщението до субекта на данните може да бъде забавено, ограничено или пропуснато, при условията и на основанията, предвидени в нормативната уредба.

Раздел IV.
Отчетност на данните.

Чл.83. (1) Администраторът е длъжен да може да докаже спазването на определените в Регламента, закона и кодекса принципи на обработване на данните.
(2) Принципът на отчетност се осигурява чрез документиране на всички основни обстоятелства относно обработването на данните съгласно Регламента.
(3) Администраторът поддържа и при поискване трябва да може да докаже и представи на Комисията и на наблюдаващия орган най - малко следните документи:

1. Списък с регистрите;
2. Анализ на риска за обработване на данните, съответно оценка на въздействието;
3. Договори с обработващи данни относно поемане на задълженията съобразно Регламента и закона;
4. Информация за субектите на данни (политика за прозрачност);
5. Образци на заявления за упражняване на правата на субектите;
6. Процедури за обработка на данните;
7. Правила за поведение на персонала относно съхранение на данните;
8. Опис на техническите средства – компютърни конфигурации и други устройства за приложение на автоматизираните системи;
9. Одитен лист за проверка на спазването на изискванията от персонала;
10. Процедури за достъп, контрол и смяна на пароли за достъп до автоматизирани системи и електронни носители на данни;
11. Регистър на нарушенията на сигурността на данните;
12. Договор за възлагане на функции на длъжностно лице по защита на данните;
13. Списъци с инструктаж на персонала и периодично обучение за обработка на лични данни;
14. Допълнителни споразумения към трудови и граждански договори на персонала с възложена дисциплинарна отговорност за неспазването им или чрез други подходящи актове, които са част от съдържанието на трудовото правоотношение;
15. Потвърждение от наблюдаващия орган за присъединяване към кодекса.

(4) Администраторът следва да съхранява посочената документация по начин, който позволява по всяко време проверка на отчетността, без да се нарушава непропорционално нормалната работа на администратора по предоставяне ВиК услуги.
(5) При съответни мотиви за това, администраторът може да поиска да представи документацията в определен разумен срок, но не повече от три работни дни.
(6) Администраторът има право да въведе други или допълнителни документи, които осигуряват изпълнението на изискванията за отчетност и позволяват контрол за спазването на съответствие с правилата на кодекса, както и да обедини документите по ал.3 в подходящи актове.

ГЛАВА ПЕТА
ПРЕДАВАНЕ НА ДАННИ И ИЗВЪНСЪДЕБНО УРЕЖДАНЕ НА СПОРОВЕ.
Раздел I .
Предаването на лични данни на трети държави или международни организации

Чл.84. (1) Предаването на данните на трети държави или международни организации се извършва при спазване на изискванията на Регламента и на закона.
(2) При предаване на лични данни в трета държава въз основа на решение на Европейската комисия за адекватно ниво на защита за тази държава не се изисква разрешение от Комисията.
(3) Европейската комисия публикува в Официален вестник на Европейския съюз и на своя уебсайт списък на трети държави, територии и конкретни сектори в трета държава и международни организации, за които е решила, че осигуряват или че вече не осигуряват адекватно ниво на защита.

Чл.85.(1) Предаване на данни в трета държава е допустимо при наличие на подходящи гаранции.
(2) подходящи гаранции могат да бъдат предвидени и без да се изисква разрешение от компетентния надзорен орган да се предават данни в случай на:
1. Наличие на акт със задължителен характер между страните по предаването на данни;
2. Одобрени от компетентния надзорен орган задължителни дружествени правила;
3. Стандартни договорни клаузи, приети от Европейската комисия;
4. Придържане на двете страни към този кодекс;
5. Одобрен механизъм за сертифициране, по който и двете страни са доказали съответствие.

Чл.86. При липса на адекватно ниво на защита или подходящи гаранции трансферирането на данни е допустимо при следните случай:
1. съгласие на субекта на данни;
2. изпълнение на договор между субекта на данните и администратора или за изпълнението на преддоговорни мерки, взети по искане на субекта на данните;
3. изпълнение на договор, сключен в интерес на субекта на данните между администратора и друго физическо или юридическо лице;
4. предаването е необходимо поради важни причини от обществен интерес;
5. предаването е необходимо за установяването, упражняването или защитата на правни претенции;

6. предаването е необходимо, за да бъдат защитени жизненоважните интереси на субекта на данните или на други лица, когато субектът на данните е физически или юридически неспособен да даде своето съгласие.

Чл.87.(1) Предаването на данни на трети лица от трети държави се извършва след информиране на субектите на данните за намерението на администратора да предаде личните данни на трета държава или на международна организация, както и наличието или отсъствието на решение на Комисията относно адекватното ниво на защита или позоваване на подходящите или приложимите гаранции и средствата за получаване на копие от тях или на информация къде са налични.
(2) В случай на липса на решение на Комисията по чл.45, §3 от Регламента, предаването на данните се извършва въз основа на договор за предаване на данни между администратора и третото лице, в който се съдържат стандантни клаузи за защита на данните, одобрени от Европейската комисия или Комисията, както и посочване на:

1. Целите на предаване на данните;
2. Категориите субекти на данните;
3. Сроковете за предаване и обработка на данните;
4. Приложими изисквания към получателя според неговата национална уредба;
5. Специални категории данни;
6. Данни за контакт на страните.

(3) Администраторът документира предаванията на основание на ал.2, включително датата и момента на предаване, информацията относно получаващия компетентен орган, обосновка на предаването и предадените лични данни.
(4) Администраторът информира компетентния надзорен орган за категориите предавания по ал.2 и при поискване й предоставя достъп до документацията.

Раздел II.
Извънсъдебни производства и процедури за разрешаване на спорове между администраторите и субектите на данни по отношение на обработването

Чл.88. (1) Без да се засягат правата на субектите на данни по Регламента и закона за подаване на жалби и съдебна защита, споровете между субекти на данните и администраторите се уреждат на доброволна основа чрез преговори.
(2) Администраторът изпраща в срок от 30 дни от получаване на искане за обезщетение или жалба от субект писмен отговор с посочване на становището и мотиви. Електронната форма се приема за приравнена писмена.
(3) Администраторът може да изиска допълнителна информация от субекта относно съставяне на становището му.
(4) Администраторът полага усилия за постигане на доброволно споразумение със субекта, което е в писмена форма и следва да съответства на закона.
(5) Администраторът може да предложи на субекта да се обърнат към медиация или към посредничеството на наблюдаващия орган за съдействие относно помирение.
(6) Администраторът е длъжен да уведоми субекта, че може да се обърне към наблюдаващия орган или към надзорния орган, съответно съдилищата, за защита на правата си по административен или съдебен ред.

Чл.89. (1) Субектите на данни могат да отправят жалба относно засягане на правата им по Регламента, закона или кодекса, както и относно искане за обезщетение, до наблюдаващия орган.
(2) Жалбата е в писмен вид и трябва да съдържа:
1. три имена на жалбоподателя;
2. адрес за кореспонденция и/или електронен адрес;
3. име на представител;
4. изложение на обстоятелствата;
5. конкретно формулирано искане;
6. подпис.
(3) Жалбите се подават по поща с писмо с обратна разписка или куриер, по електронен път или факс.
(4) Към жалбата се прилагат доказателства, каквито субектът разполага, за доказване на твърденията му.
(5) За разглеждане на жалбата не се изисква такса или възнаграждение за наблюдаващия орган.
(6) Наблюдаващият орган не е страна по производството, не носи отговорност за действията на администраторите, присъединили се към този кодекс, и няма правомощия да присъжда обезщетения или разноски на субектите.
(7) Субектите на данни може да се представляват от нарочно упълномощено лице с изрично писмено пълномощно.
(8) В едноседмичен срок от получаване на жалбата наблюдаващия орган определя докладчик, който да състави становище.
(9) Докладчикът изпраща препис от жалбата за отговор на администраторът в срок от 30 дни.
(10) След изтичане на срока за отговор, докладчикът изготвя становище по случая.
(11) Жалбата се разглежда от едночленен или тричленен състав от представители на наблюдаващия орган. Съставът може да покани субекта и администратора лично да представят обяснения или допълнителни доказателства.
(12) Съставът се произнася с мотивирано решение в срок от 30 дни от изтичане на срока за отговор като:
1. Установява нарушение на кодекса;
2. Налага санкция на администратора по кодекса;
3. Предлага на страните да се обърнат към медиация, като им предлага проект на споразумение между тях.
(13) Решението се подписва от представителите на наблюдаващия орган.
(14) Наблюдаващия орган води регистър на всички преписки и решения от състави.

Чл.90.(1) Наблюдаващият орган не предоставя консултации на субектите на данни с изключение на предвиденото в този кодекс.
(2) Наблюдаващият орган оказва съдействие на субектите на данни за подаване на жалби до надзорния орган чрез информация за контакти и правото му на жалба.

ГЛАВА ШЕСТА

ПРИСЪЕДИНЯВАНЕ, ВРЕМЕННО СПИРАНЕ И ПРЕКРАТЯВАНЕ НА ПРИЛАГАНЕТО НА КОДЕКСА. НАБЛЮДАВАЩ ОРГАН.

Раздел I.

Присъединяване към кодекса.

Чл.91. (1) Присъединяването към кодекса се извършва с писмено заявление по образец, утвърден от наблюдаващия орган.
(2) Към кодекса могат да се присъединят членове на сдружение СВКОРБ и други оператори на ВиК услуги, които се задължават да спазват настоящия кодекс.
(3) В заявлението се посочва ЕИК на кандидата или препис от документ за актулна регистрация, издаден от друга държава.
(4) Наблюдаващият орган разглежда заявленията по реда на постъпването им.
(5) В случай, че заявителят отговаря на условията, наблюдаващият орган определя срок за заплащане на възнаграждение за проверка на условията и изискванията за внедряване на кодекса.
(6) След заплащане на възнаграждението, определени от наблюдаващия орган лица извършват проверка на готовността на администратора за спазване на кодекса.

Чл.92. (1) При положително становище от проверката на дейността по обработка на данни и внедряване на изискванията на кодекса, наблюдаващият издава акт за присъединяване на администратора към кодекса.
(2) Наблюдаващият води регистър на присъединилите се към кодекса лица, който съдържа номер на администратора и данни за контакти с него. При поискване наблюдаващият орган удостоверява пред Комисията, че даден администратор се е присъединил към кодекса и го спазва, съответно наличието на нарушения и жалби срещу него.
(3) Наблюдаващият орган публикува на интернет страницата си името и адреса на ВиК операторите, които са се присъединили към прилагане на кодекса.
(4) На видно място в помещенията на администратора или на интернет страницата му се поставя знак по образец, утвърден от наблюдаващия орган, че доставчикът се е присъединил и прилага кодекса.

Чл.93. (1) Най-малко веднъж годишно администраторът доказва пред наблюдаващия орган съответствието на дейността му с кодекса и документите по внедряване на изискванията за спазването му.
(2) При наличие на пропуски или липса на отчетност, наблюдаващият орган съдейства на администраторите за отстраняването им, съответно изпълнение на изискванията на кодекса.

Чл.94. (1) Проверките по реда на кодекса се извършват от определени от наблюдаващия орган лица.
(2) Администраторът е длъжен да предостави съдействие на наблюдаващия орган чрез предоставяне на документи и достъп до автоматизирани системи за обработка на данни, достъп до помещенията на администратора, предоставяне на обяснения и становища и други подходящи мерки.
(3) Всички предписания и препоръки за спазване на настоящия кодекс са задължителни за администраторите, като наблюдаващият орган определя разумни срокове за това.

(4) Присъединяването и прилагането на кодекса, съответно заплащане на определените от наблюдаващия орган възнаграждения за внедряване и поддържане на системата на отчетност, са доброволни. Администраторът има право да се откаже от прилагане на кодекса, като изпрати уведомление за това на наблюдаващия орган.

Раздел II.
Временно спиране (суспендиране), прекратяване и изключване от приложение на кодекса.

Чл.95. (1) Администраторите имат право с надлежно уведомление и при липса на парични задължения към наблюдаващия орган временно да спрат прилагане на кодекса с посочване на причините за това.
(2) Наблюдаващият орган има право да постанови временно спиране на приложението на кодекса, ако след проверка се установи, че администраторът не отговаря на изискванията му. Наблюдаващият орган определя срок за изпълнение на предписанията.
(3) Наблюдаващият орган отбелязва в регистъра временното спиране на приложение на кодекса.

Чл.96. (1) Администраторите имат право с надлежно уведомление и при липса на парични задължения към наблюдаващия орган да прекрати прилагане на кодекса с посочване на причините за това.
(2) Наблюдаващият орган има право да постанови изключване на приложението на кодекса, ако след проверка се установи, че администраторът е извършил нарушение на правилата на кодекса.
(3) Наблюдаващият орган отбелязва в регистъра изключване от приложение на кодекса.

Чл.97. При запитване от страна на Комисията наблюдаващият орган посочва началната и крайна дата на прилагане на кодекса от ВиК оператор, съответно – периоди на спиране на прилагането му.

Чл.98. (1) Наблюдаващият орган има право да издаде мотивирано решение за изключване или спиране прилагането на кодекса при установени нарушения или несъответствие с изискванията му.
(2) Спиране от прилагане на кодекса за период от един до шест месеца се постановява :
1. в случаите по чл.95, ал.2;
2. при неизпълнение на предписание на наблюдаващия орган;
3. при нарушение на кодекса.

(3) Изключване от прилагането на кодекса се постановява при:
1. неизпълнение на предписание на наблюдаващия орган, продължило след срока на спиране на прилагането на кодекса;
2. тежко нарушение на кодекса.

(4) Тежко нарушение на кодекса съставлява:
1. немотивиран отказ за прилагане на правата на субектите;
2. отказ за участие в извънсъдебно уреждане на спорове по глава Пета;
3. деклариране и отчитане на неверни данни и обстоятелства относно въведените технически и организационни мерки за защита на данните;

4. неуведомяване на Комисията и на наблюдаващия орган при нарушение на сигурността на данните;
5. неправомерно обработване на лични данни без съгласие на субектите и без правно основание;
6. неизпълнение на задълженията за заплащане на възнаграждения за внедряване на система за приложение на кодекса;
7. уронване престижа и разпространение на неверни данни относно наблюдаващия орган;
8. предоставяне на лични данни на трети лица, включително в трети държави и международни организации, в нарушение на определения в Регламента, закона и кодекса ред;
9. неизпълнение на второ или последващо предписание на наблюдаващия орган;
10. неоказване на съдействие чрез предоставяне на информация и достъп до помещенията на администратора за извършване на проверки за спазване на кодекса;
11. отказ за участие и предоставяне на данни и доказателства в производствата за извънсъдебно решаване на спорове по кодекса;
12. неизпълнение на решение на наблюдаващия орган, поставено в производството по извънсъдебно решаване на спорове;
13. препятстване на ефективното упражняване на правомощието по наблюдение по друг начин.

(5) Наблюдаващият орган уведомява Комисията за решенията за спиране или изключване от прилагане на кодекса и предоставя информация за тях.

Раздел III.
Наблюдаващ орган

Чл.99. (1) Сдружение Съюз на ВиК операторите в Република България (сдружението)изпълнява правомощията на наблюдаващ орган по този кодекс.
(2) Управителният съвет на сдружението приема процедури за наблюдение на приложението на кодекса по смисъла на чл.41, §2 от Регламента, които са публични на интернет страницата на сдрежението и се изпращат на Комисията.

Чл.100. (1) При изпълнение на правомощията си на наблюдаващ орган сдружението е независимо и избягва конфликт на интереси.
(2) С оглед предотвратяване на конфликт на интереси се прилагат следните мерки:
1. в проверките за прилагане на кодекса и текущо оценяване не участват членове на органите на сдружението, които се явяват свързани лица с администратора или с обработващ данни от името на администратора;
2. в съставите за решаване на извънсъдебните производства за уреждане на спорове по кодекса не участват лица, които се явяват свързани лица със субекта на данните или администратора или с обработващ данни от името на администратора;
3. при наличие на данни или информация за обстоятелства, които поставят под съмнение обективността и безпристрастността на лицата, определени от наблюдаващия орган за извършване на проверки относно спазването му и съдействие на администраторите, наблюдаващият орган определя други лица;

4. определените от наблюдаващия орган лица, които извършват дейности по този кодекс, не получават възнаграждения по граждански или трудови договори от администраторите на лични данни, които проверяват;
5. наблюдаващият орган няма участие в капитала на администраторите и не определя техните управителни органи;
6. администраторите и обработващите данни не определят и нямат пряко влияние върху избора на управителни органи на наблюдаващия орган;
7. наблюдаващият орган няма договори с администраторите за обработка на лични данни.

ГЛАВА СЕДМА
ИЗМЕНЕНИЕ И ДОПЪЛНЕНИЕ НА КОДЕКСА. ПРИЛАГАНЕ БЕЗ АКРЕДИТИРАН НАБЛЮДАВАЩ ОРГАН.
Раздел I.
Изменение и допълнение на кодекса

Чл.101. (1) Настоящият кодекс се изменя и допълва от Управителния съвет на сдружението по реда на приемане на решения от УС на сдружението съобразно Закон за юридическите лица с нестопанска цел и Устава му.
(2) Предложения за изменение и допълнение на кодекса могат да бъдат правени от :
1. членове на УС на сдружението;
2. членове на сдружението;
3. субекти на данни и техни представителни организации.
(3) Проектът за изменение и допълнение на кодекса се изготвя от УС на сдружението или създадена към него работна група.
(4) Проектът се публикува за обществено консултиране от най – малко 14 дни на интернет страницата на сдружението.
(5) Веднъж годишно се извършва преглед на съдържанието на кодекса за съответствие с промени в нормативната уредба или с развитието на обществените отношения. УС на сдружението изготвя проект за изменение и допълнение на кодекса съобразно резултата от проверката.

Чл. 102. (1) Приетият от УС на сдружението проект на изменение и допълнение на кодекса се внася за одобрение пред надзорния орган с придружително писмо и посочени мотиви за изменението или допълнението.
(2) След одобряване на кодекса от надзорния орган, той се публикува на интернет страницата на сдружението с посочване на датата на прилагане на измененията.
(3) Ако не е посочено друго измененията и допълненията на кодекса влизат от деня на публикуване на кодекса на интернет страницата на надзорния орган по реда на чл. 40, §6 от Регламента, като присъединените администратори имат срок от 30 дни да приведат дейността си в съответствие с измененията и допълненията.
(4) При неизпълнение на изискванията по ал.3 от администраторите, наблюдаващият орган може да приложи временно спиране от прилагане на кодекса до изпълнение на изискванията му.

Раздел II.

Прилагане на кодекса без наблюдаващ орган.

Чл.103. (1) Настоящият кодекс се прилага и в случаите на одобряването му от страна на надзорния орган и липса на акредитиране на сдружението като наблюдаващ орган.
(2) Администраторите се задължават самостоятелно да приведат дейността си в съответствие с кодекса и да поддържат всички доказателства за изпълнението на кодекса.
(3) Администраторите се задължават да документират хронологично доказателства относно първоначална проверка за изпълнението на изискванията на кодекса и последваща годишна проверка.
(4) Проверките могат да се извършват от длъжностно лице за защита на данните на администратора, друг служител на администратора, натоварен с тези функции или външно независимо лице, включително представители на сдружението по определени от сдружението правила.

Чл.104. (1) Администраторите оповестяват по подходящ начин решението си да прилагат кодекса и началната дата на прилагането му.
(2) Подходящ начин за оповестяване е посочване на интернет страницата на администратора, чрез включване на информация в политиката (декларация) за конфиденциалност и чрез поставяне на съобщения на интернет страницата на сдружението.
(3) Администратор, който прилага кодекса, се задължава да предоставя на субектите по ясен и разбираем начин информация за съдържанието на кодекса чрез предоставяне на екземпляри от него или по друг начин.

Чл.105. (1) Администраторите се задължават да полагат усилия за доброволно уреждане на спорове със субектите, като се обърнат, при наличие на съгласие от страна на субектите, към съдействие и консултации от страна на сдружението или към медиация.
(2) Правилата на ал.1 не препятстват упражняването от субектите на предоставените им със закон права на жалби и обезщетения по съдебен ред.

Чл.106. След акредитиране на сдружението като наблюдаващ орган, администраторите имат право да се откажат да прилагат кодекса, като присъединяването им се извършва според разпоредбите на кодекса и одобрените правила по чл.41, §2, б.“б“ от Регламента.

ДОПЪЛНИТЕЛНА РАЗПОРЕДБА

§1. Следните понятия имат определения смисъл по този кодекс:

1. „Комисията“ - Комисия за защита на личните данни по глава Втора от Закон за защита на личните данни;
2. "Наличност" е изискване за осигуряване непрекъсната възможност за обработване на личните данни на оторизираните лица и за изпълнение на функциите на системата за обработване или бързото им възстановяване;
3. "Постоянна поверителност" е изискване за текущо и постоянно гарантиране на неразкриване на личните данни на неоторизирани лица в процеса на тяхното обработване;

4. "Потребители" са:
   а) юридически или физически лица - собственици или ползватели на съответните имоти, за които се предоставят ВиК услуги;
   б) юридически или физически лица - собственици или ползватели на имоти в етажната собственост;
   в) предприятия, ползващи вода от водоснабдителните мрежи на населените места за технологични нужди или подаващи я на други потребители след съответна обработка по самостоятелна водопроводна инсталация, непредназначена за питейни води.
   "Нов потребител" е:
   а) възложител на строеж, който се предвижда да бъде присъединен към водоснабдителната и/или канализационната система;
   б) възложител на реконструкция, преустройство или смяна на предназначение на съществуващ, присъединен към водоснабдителната и/или канализационната система, обект;
   в) купувач на съществуващ и присъединен към водоснабдителната и/или канализационната система обект.
5. „Регламента“ - 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;
6. „Риск“ - възможността за настъпване на имуществена или неимуществена вреда за субекта на данните при определени условия, оценени от гледна точка на тяхната тежест и вероятност;
7. "Свързани лица":
– съпрузите, роднините по права линия - без ограничения, по съребрена линия - до четвърта степен включително, и роднините по сватовство - до трета степен включително;
– работодател и работник;
– лицата, едното от които участва в управлението на дружеството на другото;
– съдружниците;
– дружество и лице, което притежава повече от 5 на сто от дяловете и акциите, издадени с право на глас в дружеството;
– лицата, чиято дейност се контролира пряко или косвено от трето лице;
– лицата, които съвместно контролират пряко или косвено трето лице;
– лицата, едното от които е търговски представител на другото;
– лицата, едното от които е направило дарение в полза на другото.
   "Свързани лица" са и лицата, които участват пряко или косвено в управлението, контрола или капитала на друго лице или лица, поради което между тях могат да се уговарят условия, различни от обичайните;
8. „Устойчивост“ е изискване системите за обработване на данни да бъдат текущо проверявани и поддържани с оглед избягване на нежелани събития с данните;
9. "Цялостност" е изискване данните да не могат да бъдат променени/подменени по неоторизиран начин в процеса на тяхното обработване и изискване да не се дава възможност за изменение и за неразрешени манипулации на функциите по обработване на данните.

ПРЕХОДНИ И ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§1. (1) Настоящият кодекс за поведение е изработен и приет от Управителния съвет на сдружение Съюз на ВиК операторите в Република България на основание чл. 40, §1 от 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 и е одобрен от Комисия за защита на личните данни на основание чл.40, §5 от Регламента.
(2) УС на сдружение Съюз на ВиК операторите в Република България е провел обсъждане и обществено консултиране на проекта на кодекс сред заинтересованите лица, които са имали възможност да представят становищата си.
§2. Кодексът влиза в сила и се прилага от администраторите и наблюдаващия орган от датата на одобряването му от Комисия за защита на личните данни и публикацията на интернет страницата на Комисията.
§3. Кодексът е заверен от председателя на Управителния съвет на сдружение Съюз на ВиК операторите в Република България и от Комисия за защита на личните данни и е публикуван на интернет страницата на сдружение Съюз на ВиК операторите в Република България.
§4. Администраторите, които са заявили намерение за присъединяване към него преди началото на приложението му привеждат дейността си в съответствие с изискванията му в срок до два месеца.
§5. Наблюдаващият орган утвърждава образците на документи по приложение на кодекса в срок до шест месеца от началото на приложението му.
§6. Наблюдаващият орган издава указания, инструкции и предписания за тълкуване и прилагане на кодекса, които се обявяват на интернет страницата на наблюдаващия орган и по друг подходящ начин на администраторите, които прилагата кодекса. Актовете на наблюдаващия орган по приложението на кодекса са задължителни за администраторите, които го прилагат.