ВЪТРЕШНИ ПРАВИЛА
за мерките за защита на личните данни в Община Несебър

I. Общи положения

Предмет

Чл. 1. Тези Вътрешни правила уреждат условията и реда за водене на регистри на лични данни, минималното ниво на технически и организационни мерки за тяхната защита, както и упражняването на контрол при обработването на лични данни в Община Несебър.

Принципи при обработване на лични данни

Чл. 2. При обработването на лични данни в Община Несебър се спазват следните принципи:

1. законосъобразност, добросъвестност и прозрачност;
2. ограничение на целите;
3. свеждане на данните до минимум;
4. точност;
5. ограничение на съхранението;
6. цялостност и поверителност;
7. отчетност.

II. Администратор и регистри с лични данни

Индивидуализиране на администратора на лични данни

Чл. 3. (1) Администратор на лични данни е Община Несебър, със седалище и адрес на управление: гр. Несебър, ул. „Еделвайс“ № 10. Адресът за кореспонденция и контакт е гр. Несебър, ул. „Еделвайс“ № 10, тел. 0554 / 29370, 43281, contacts@nesebar.bg, www.nesebarinfo.com.

(2) В Община Несебър се обработват лични данни във връзка със спазване на законови задължения и изпълнение решенията на Общински съвет – Несебър, като ръководството на общината определя целите и средствата за обработването им, при спазване на относимите нормативни актове.

(3) Личните данни се обработват самостоятелно от администратора на лични данни и чрез възлагане на обработващи лични данни.

(4) Обработващите лични данни са описани в Приложение № 1 към настоящите Правила;

(5) Кметът на Община Несебър определя длъжностно лице по защита на данните, което да отговаря за координиране и прилагане на мерките за защита на личните данни.

Условия за достъп до лични данни

Чл. 4. 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” и след запознаване с нормативната уредба в областта на защитата на личните данни, политиката за защита на личните данни и опасностите за личните данни, обработвани от администратора, като за целта в длъжностната характеристика на служителите се вписва отговорност за гарантиране поверителността при работа с лични данни.

Права на физическите лица при обработване на отнасящи се за тях лични данни

Чл. 5. (1) Всяко физическо лице, чийто лични данни ще се обработват от Община Несебър, следва да бъде уведомено за:

1. данните, които идентифицират Община Несебър;

2. целите на обработването на личните данни и правното основание за обработването;

3. категориите лични данни, отнасящи се до съответното физическо лице;

4. получателите или категориите получатели, на които могат да бъдат разкрити данните;

5. срока за съхранение на личните данни;

6. информация за правото на достъп и правото на коригиране, изтриване или ограничаване на обработването на събраните данни, правото на възражение и правото на преносимост при условията на Регламент (ЕС) 2016/679 – Общия регламент относно защитата на данните;

7. право на оттегляне на съгласието по всяко време, когато обработването на личните данни се основава на съгласие на лицето;

8. правото на жалба до Комисията за защита на личните данни;

9. източника на данните;

10. съществуване на автоматизирано вземане на решения, включително профилиране.

(2) Информацията по ал. 1 се обявява на видно място в офисите на Центъра за административно и информационно обслужване, в дирекция „Транспорт“, на официалната интернет страница на общината.

(3) Служителите на Община Несебър попълват декларация за информираност и съгласие за обработване на лични данни за целите на трудовото/служебното правоотношение. Декларацията се съхранява в досието на служителя в отдел „Човешки ресурси и ТРЗ“.

(4) Алинея 1 не се прилага, когато:

1. обработването е за статистически, исторически или научни цели и предоставянето на данните по ал. 1 е невъзможно или изисква прекомерни усилия;

2. вписването или разкриването на данни са изрично предвидени в закон;

3. физическото лице, за което се отнасят данните, вече разполага с информацията по ал. 1;

4. е налице изрична забрана за това в закон.

(5) Достъп на лица до личните им данни се предоставя, след подаване на писмено заявление до кмета на община Несебър в 30-дневен срок от подаване на заявлението.

Поддържани регистри на лични данни

Чл. 6. В Община Несебър се обработват лични данни в следните регистри:

1. Регистър „ГРАО“ – ЛБ Население – Картотечен регистър; Актове за раждане; Актове за брак; Актове за смърт;
2. Регистър „Деловодство“;
3. Регистър „Настойничество и попечителство“;
4. Регистър на категоризираните туристически обекти от кмета на общината по чл. 128 от Закона за туризма;
5. Регистър „Транспорт“ – Разрешения за таксиметров превоз, Карти за паркиране на хора с трайни увреждания и Пропускателен режим, паркинги и паркоместа;
6. Регистър „Търговия“ – Разрешения за поставяне на РИЕ и Разрешения за търговия на открито;
7. Регистър „Устройство на територията“ – Разрешения за строеж; Удостоверения за въвеждане в експлоатация; Технически паспорти на сгради;
8. Регистър „Контрол върху строителството“ – Актове за узаконяване, Удостоверения за търпимост и преписки за незаконни строежи;
9. Регистър „Разрешения за прокопаване“;
10. Регистър „Етажна собственост“ – Сдружения на собственици в сгради, в режим на етажна собственост и регистър- справка по чл. 46 „б“ от ЗУЕС;

11. Регистър „Общинска собственост“ – Главни регистри за общинска собственост – публична и частна, Регистър на разпоредителните сделки с имоти – общинска собственост, Регистър на договорите за наем на имоти – общинска собственост и регистър Картотекиране;
12. Регистър „Местни данъци и такси“;
13. Регистър „Човешки ресурси“ /кандидати за работа; персонал – трудови и служебни правоотношения, болнични листи, трудови злополуки/;
14. Регистър „Административно наказателни преписки“;
15. Регистър „Съдебни дела“;
16. Регистър на МКРППМН;
17. Регистър „Еднократни финансови помощи“;
18. Регистър „Персонални пенсии по чл. 92 от КСО“;
19. Регистър „Контрагенти“ /доставчици, клиенти, граждански договори/;
20. Регистър „Договори за безвъзмездна финансова помощ“;
21. Регистър „Екология“
22. Регистър „Общински съвет Несебър“ /преписки/;
23. Регистър на извършените одитни ангажименти от ЗВО“;
24. Регистър „Пропускателен режим“;
25. Регистър „Видеонаблюдение“;
26. Регистър „Нотариални заверки“.

Чл. 7. (1) Общо описание на всеки регистър, категории лични данни, основание за обработване, носителите на данни, технология на обработване, срока за съхраняване, оценка на въздействието и определяне съответното ниво на защита, длъжностните лица, които работят с данните са описани в Приложение № 2.

(2) Нивото на въздействие на регистрите е определено по следните критерии:

1. поверителност;
2. цялостност;
3. наличност.

Технически и организационни мерки за защита на личните данни

Чл. 8 (1) Физическата защита на личните данни се осъществява при спазване на следните мерки:

1. Достъпът на външни лица в сградата на Община Несебър е ограничен с пропускателен режим. На входа на административната сграда има жива охрана и видеонаблюдение. Всеки служител има персонална магнитна карта за достъп.

2. Извън работното време на Община Несебър, сградата се заключва. Осигурено е 24 часово дежурство от Общинския съвет за сигурност. Офисите на ЦАИО и изнесените офиси се охраняват със СОТ система.

3. Личните данни се обработват в ЦАИО и кабинетите на служителите.

4. Работните места в ЦАИО са организирани по подходящ начин за временното съхраняване на документи на хартиен носител, съдържащи лични данни, скрити от потребителите на услуги.

5. Всички документи на хартиен носител, съдържащи лични данни, се съхраняват в шкафове, единствено в кабинетите на служителите, които са упълномощени да работят с тях. Разположените шкафове за съхранение на документи в коридорите на сградата са метални и се заключват, като с ключ разполагат само упълномощени служители.

6. Помещенията, в които се обработват лични данни са оборудвани с заключване на вратите и пожарогасителни средства.

7. Външни лица имат достъп до помещенията, в които се обработват лични данни, само в присъствието на упълномощени служители.

8. Учрежденският архив е осигурен с охранителна система СОТ и достъп до него има единствено архиваря на общината.

(2) Персоналната защита на личните данни се осъществява при спазване на следните мерки:

1. Лицата, обработващи лични данни, се запознават с Регламент (ЕС) 2016/679, ЗЗЛД, настоящите Вътрешни правила, Номенклатурата на делата за срокове за съхраняване в Община Несебър.

2. Лицата, обработващи лични данни, преминават обучение, включващо запознаване с политиката на Община Несебър за защита на личните данни, запознаване с опасностите за личните данни, обработвани в общината.

3. Лицата, обработващи лични данни, като подписват длъжностната си характеристика, поемат задължение за неразпространение на лични данни, станали им известни във връзка и по време на служебните им задължения. Екземпляр от длъжностната характеристика се съхранява в досието на всеки служител.

4. Споделяне на критична информация между служителите (като идентификатори, пароли за достъп и т.н.) е забранено.

5. Служителите, на които е възложено да подписват служебна кореспонденция с универсален електронен подпис /УЕП/, нямат право да предоставят издадения им УЕП на трети лица.

(3) Документалната защита на обработваните лични данни се осъществява при спазване на следните мерки:

1. Лични данни в Община Несебър постъпват основно на хартиен носител (заявления, искания, в едно с изискуемите нормативно документи), а отделни дейности по обработване на данните налагат поддържане на данни в електронен вид.

2. Обработването на личните данни се извършва в рамките на работното време на общината.

3. Достъп до регистрите имат лицата, съгласно Приложение № 2 в съответствие с принципа „Необходимост да се знае”.

4. Личните данни се събират само с конкретна цел, в съответствие с нормативните изисквания към Община Несебър. Данните се класифицират в съответствие с тяхното предназначение и характер и се съхраняват шкафове в зоните с ограничен достъп.

5. Всеки ръководител на структурно звено е отговорен за контрола на достъпа до регистрите, които се поддържат в звеното.

6. Архивирането на документи се извършва при спазване на Вътрешните правила за дейността на учрежденския архив, които са съгласувани с Държавен архив – Бургас. Ръководителите на структурни звена отговарят за предаването на документите за съхраняване в учрежденския архив с приемо-предавателен протокол по образец, подписан от архиваря на общината.

9. 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 държавни органи или упълномощени лица.

10. Временните документи от регистъра, които са на хартиен носител и съдържат лични данни, се унищожават само чрез специално устройство (шредер).

(4) Защитата на автоматизирани информационни системи и мрежи се осъществява при спазване на следните мерки:

1. При работа с данните от регистрите се използват съответните софтуерни продукти за обработване. Данните се въвеждат в база данни и се съхраняват на сървър. Всеки упълномощен служител има личен профил (потребителско име и парола), с определени съобразно задълженията му права и нива на достъп. Дефинирани са и уникални потребителски имена и пароли за стартиране на операционната система на всеки един компютър.

2. Администраторът създава и поддържа стандартни и сигурни конфигурации за всяка компютърна и мрежова платформа, с която оперира, което включва стандартни и базови конфигурации за защита на операционната система, защитни стени, рутери и мрежови устройства. За защита на данните е инсталирана антивирусна програма и се извършва периодична профилактика на софтуера и системните файлове.

3. Ръководителят на структурното звено е отговорен за управлението на регистрите в съответното звено. Само съответните лицата, посочени в Приложение № 2 имат достъп до регистрите.

4. За всички компютърни конфигурации, сървъри и комуникационни средства, от които зависи правилното поддържане на базите данни, са осигурени непрекъсваеми токозахранващи устройства (UPS).

5. Помещенията, в които са разположени компютърни и комуникационни средства се заключват.

6. Организационни мерки за гарантиране нивото на сигурност:

а) Забранено е използването на преносими лични носители на данни.

б) Работните компютърни конфигурации, както и цялата IT инфраструктура, включително и достъпът до интернет, се използват единствено за служебни цели.

в) При ремонт на компютърна техника, на която се съхраняват лични данни, предоставянето й на сервизната организация се извършва без устройствата, на които се съхраняват лични данни.

8. Разрешава се осъществяването на отдалечен достъп до данни от регистрите единствено на софтуерните фирми, които са обработващ лични данни за Община Несебър и при спазване на строга конфедициалност, заложена в договорните отношения.

9. Достъп до електронните услуги, предоставяни от община Несебър се извършва чрез:

а) универсален електронен подпис;

б) единен граждански номер ведно с регистрационен номер и дата на входящ документ, подаден от лицето с този ЕГН.

(5) Криптографската защита при предаване на данни по електронен път или на преносими технически носители се осъществява чрез използване на стандартни технологии за криптиране на данните, както и използване на електронен подпис.

Действия за защита при аварии, произшествия и бедствия

Чл. 9. (1) При възникване и установяване на инцидент, веднага се докладва на длъжностното лице за защитата на личните данни.

(2) 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, упълномощено лице вписва в дневника последствията от инцидента и мерките, които са предприети за отстраняването им.

Предоставяне на лични данни на трети лица

Чл. 10. (1) Данни от регистрите могат да бъдат предоставяни на държавни институции с оглед изпълнение на нормативно задължение (НОИ, НАП, МВР и т.н.).

(2) В качеството си на работодател, Община Несебър предоставя лични данни и на определени кредитни институции (банки) във връзка с изплащането на дължимите възнаграждения на служители и изпълнители по граждански договори. Личните данни, които се предоставят, са три имена и единен граждански номер и се предоставят с цел идентификация на лицето, в чиято полза се извършва плащането. Това се налага, с оглед изискванията на кредитните институции във връзка с извършваните от тях банкови преводи.

(3) Във връзка с използването на пощенски и куриерски услуги – приемане, пренасяне и доставка и адресиране на пратките до физически лица деловодителите посочват следните данни: три имена, адрес, област, пощенски код и наименование на населеното място.

Срок за провеждане на периодични прегледи относно необходимостта от обработване/заличаване на данните

Чл. 11. Всеки ръководител на структурно звено трябва да извършва ежегодни проверки на личните данни от регистрите, които се водят в звеното с оглед преценка на необходимостта от тяхното обработване, предаване за съхраняване в учрежденския архив и съответно ако е отпаднало задължението за обработване – за заличаването им.

Ред за преустановяване обработването на лични данни

Чл. 12. (1) След изтичане на срока за съхранение на данните Постоянно действащата експертна комисия (назначена със заповед на кмета на общината) определя кои документи подлежат на унищожение и мястото на извършване на процедурата.

(2) Унищожаването се извършва посредством няколко начина, определени в зависимост от наличните към момента на унищожението технически възможности за Община Несебър, а именно: чрез разрязване с помощта на машина – шредер или чрез изгаряне, или разрушаване (отваряне) на корпуса на носителя на данни.

(3) В случай на прехвърляне на данните на друг администратор е необходимо да се уведоми КЗЛД, ако прехвърлянето е предвидено в закон и е налице идентичност на целите на обработването и се съставят съответно приемо-предавателни протоколи.

ЗАКЛЮЧИТЕЛНА РАЗПОРЕДБА

Параграф единствен. Вътрешните правила се приемат на основание чл.24, параграф 1 от Регламент (ЕС) 2016/679 – Общия регламент относно защитата на данните и чл. 23, ал. 4 от Закона за защита на личните данни.

Вътрешните правила са утвърдени от кмета на Община Несебър със заповед № 996/14.06.2018г. и допълнени със заповед № 618/23.04.2019г.

Приложение № 1 Обработващи лични данни в Община Несебър

Приложение № 2 Описание на водените регистри в Община Несебър