



УТВЪРЖДАВАМ:

**ГЕОРГИ ГЕОРГИЕВ
КМЕТ НА ОБЩИНА ДЪЛГОПОЛ**

**ПРАВИЛНИК ЗА СЪХРАНЯВАНЕ И
УНИЩОЖАВАНЕ
НА ДАННИ НА ФИЗИЧЕСКИ ЛИЦА**

Общи разпоредби

Чл.1. Настоящият правилник се прилага при обработването на всички видове лични данни на физически лица извършвано от Община Дългопол.

Чл.2. Настоящият правилник е задължителен за всички служители и работници в Община Дългопол, оправомощени за работа с лични данни на физически лица.

Основни роли и отговорности

Чл. 3. (1) Длъжностното лице по защита на данните е отговорно за спазване на настоящия правилник и Инструкцията за обработване и защита на лични данни.

(2) Специалист „Човешки ресурси“ е пряко отговорен за събирането и съхранението на хартиен носител на личните данни на работниците и служителите.

(3) Пряко отговорни за събирането и съхранението на хартиен носител на личните данни на физически лица ползващи административни услуги от Община Дългопол са лицата определени със Заповед на Кмета на община за всеки един отдел.

(4) Системните администратори са пряко отговорни за събирането и съхранението на всички лични данни на физически лица на електронен носител.

Форми на водене и съхраняване на личните на данни

чл.4. (1) На хартиен носител:

1. Формата на организация и съхраняване на личните данни е писмена;
2. Местонахождението на шкафове, съдържащи документи, е в отделно помещение с ограничен достъп, като шкафове се заключват;
3. Форми за предоставяне на данните от физическите лица: лично от субекта на данните и/или от трета страна.
4. Личните данни от лицата се подават на администратора на лични данни и оправомощеното лице, назначено за обработването им.
5. Достъп до личните данни имат само оправомощените лица.

(2) На технически носител:

1. Форма на организация и съхраняване на личните данни – личните данни се съхраняват на твърди дискове, на служебни компютри с ограничен достъп, чрез персонални права за достъп до системите, съгласно задълженията по длъжностна характеристика;

2. Достъп до личните данни и защита - достъп до операционната система, съдържаща файлове за обработка на лични данни, имат само обработващите лични данни, чрез лична парола за достъп до софтуера.

3. Форма на въвеждане на данните от физически лица:

- ръчно въвеждане от оправомощеното лице чрез съответния софтуер за работа.

Чл.5. Най-малко един път годишно длъжностното лице по защита на данните извършва проверка за изтекли срокове за съхранение на налични писмени документи, съдържащи лични данни, заедно с:

- завеждащ личен състав, относно трудовите досиета на настоящи и бивши работници и служители, и всякакви други документи съдържащи лични данни на тази категория физически лица;

- определеното от Кмета на общината отговорно лице за всеки един отдел относно всякакви документи съдържащи лични данни физически лица, ползвали услугите предоставяни от АЛД.

Чл.6. (1) При констатирано наличие на документи с изтекъл срок на съхранение длъжностното лице по защита на данните, заедно със завеждащ личен състав или отговорното лице, образуват комисия, която унищожава всички документи с изтекъл срок на съхранение, чрез нарязване на шредер машина.

(2) За изпълнението на процедурата по предходната алинея се съставя Протокол за унищожаване, в който се записват датата на изпълнение, видът на унищожените документи и методът на унищожаване. Протоколът се разписва от лицата извършили проверката и процедурата по унищожаване.

(3) Протоколите за унищожение се запазват в архивна папка.

Чл.7. Най-малко един път годишно длъжностното лице по защита на данните извършва проверка за изтекли срокове за съхранение на налични писмени документи, съдържащи лични данни, заедно със системен администратор, извършват проверка за изтекли срокове за съхранение на лични данни съдържащите на електронен носител.

Чл.8. (1) При констатирано наличие на лични данни с изтекъл срок на съхранение длъжностното лице по защита на данните, заедно със системния администратор, образуват комисия, която изтрива всички данни с изтекъл срок на съхранение.

(2) При техническа възможност се създава „лог“ файл съдържащ данни за извършените действия, който следва да се разпечата и на харитен носител,

и се подпише от системния администратор и длъжностното лице по защита на данните.

(3) При липса на техническа възможност за създаване на нарочен файл, съдържащ данните за извършените действия, се съставя Протокол за изтриване, в който се описват датата на изпълнение, видът на изтрите данни и методът на изтриване. Протоколът се разписва от лицата извършили проверката и процедурата по унищожаване.

(4) Протоколите за унищожаване и/или разпечатаните „лог файлове” се запазват в архивна папка. Лог файловете се пазят и в електронен вариант в нарочна папка на хард диск.