Регионална библиотека "Ем. Попдимитров"
гр. Кюстендил

☎: *078/55 01 16 Директор* ☎: *078/55 01 19 Заемна за възрастни*

ул. "Л. Каравелов" № 1 ☎: *078/55 01 17 Счетоводство*

ИЗВАДКА

И Н С Т Р У К Ц И Я

за обработване на лични данни и защитата им от незаконни форми на обработване в регистрите, съгласно изискванията на Закона за защита на личните данни, водени в Регионална библиотека „Ем. Попдимитров"

I. ОБЩИ ПОЛОЖЕНИЯ

Чл. 1. Настоящата инструкция има за цел да регламентира:

- ✓Механизмите за защита на личните данни, обработвани от Регионална библиотека „Ем. Попдимитров" в качеството й на Администратор на лични данни (АЛД)
- ✓Определяне на длъжностните лица, обработващи лични данни и/или лицата, които имат достъп до лични данни и работят под ръководството на обработващите лични данни, както и тяхната отговорност при неизпълнение на тези задължения, свързани с обработване и защита на лични данни, правата и задълженията им.
- ✓Оценката на въздействието и определяне нивото на защита на регистрите с лични данни, поддържани от Регионална библиотека „Ем. Попдимитров".
- ✓Необходимите технически и организационни мерки за защита на личните данни от неправомерно обработване (случайно или незаконно унищожаване, случайна загуба, неправомерен достъп, изменение или разпространение), както и всички други незаконни форми на обработване на лични данни.
- ✓Действия за защита при аварии, произшествия и бедствия.
- ✓Правилата за предоставяне на лични данни на трети лица.
- ✓Сроковете за провеждане на периодични прегледи относно необходимостта от обработване на данните, както и заличаването им.
- ✓Реда за унищожаване или предоставяне на данните на друг администратор.

II. ИНДИВИДУАЛИЗИРАНЕ НА АДМИНИСТРАТОРА И ОБРАБОТВАЩИТЕ ЛИЧНИ ДАННИ

Чл. 2 (ал.1) Индивидуализиране на администратора на лични данни.

Данни за АЛД от Регистър БУЛСТАТ към Агенция по вписванията:

- Код по Булстат XXXXXX
- Фирма, правна форма : Регионална библиотека, юридическо лице
- Седалище и адрес на управление : Кюстендил, 2500, ул. „Л. Каравелов“ 1
- Тел. 078 550116
- Директор : София Пейчева

(2) Регионалната библиотека в качеството си на АЛД е вписана в Регистъра на администраторите на лични данни и на водените от тях регистри на лични данни, поддържан от Комисията за защита на личните данни (КЗЛД) с идентификационен номер **0053978**

(3) АЛД обработва личните данни самостоятелно и чрез възлагане на обработващ данните

(4) АЛД може да определи едно или повече лица с право на достъп до лични данни, които да отговарят за координиране и прилагане на мерките за защита.

(5) 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 и ръководствата за защита на личните данни, обработвани от администратора, като за целта лицата подписват декларация за неразгласяване на лични данни, до които са получили достъп при и по повод изпълнение на задълженията си. (Приложение 3)

(6) Всички лица отговарят за спазването на ограниченията за достъп до личните данни и са персонално отговорни пред Директора за нарушаване на принципите за поверителност, цялостност и наличност на личните данни, освен в случаите на форсмажорни обстоятелства.

(7) Всяко физическо лице, чийто лични данни ще се обработват от администратора, следва да бъде уведомено за :

- данните, които идентифицират администратора;
- целите на обработването на личните данни;
- категориите лични данни, отнасящи се до съответното физическо лице;
- получателите или категориите получатели, на които могат да бъдат разкрити данните;
- информация за правото на достъп и правото на коригиране на събраните данни.

(8) Когато личните данни не са получени от физическото лице, за което те се отнасят, ал. 7 не се прилага, ако :

- обработването е за статистически, исторически или научни цели и предоставянето на данните по ал. 1 е невъзможно или изисква прекомерни усилия;
- вписването или разкриването на данни са изрично предвидени в закон;

- Физическото лице, за което се отнасят данните, вече разполага с информацията по ал.1;
- е налице изрична забрана за това в закон.

.....

III. ОБЩО ОПИСАНИЕ НА ПОДДЪРЖАНИТЕ РЕГИСТРИ

Чл. 3. *РЕГИСТЪР „ПОТРЕБИТЕЛИ“*

В Регистър „Потребители“ се обработват лични данни, свързани с потребителите-читатели, посетители на Регионална библиотека „ Ем. Попдимитров“. В качеството си на Администратор на лични данни, Регионалната библиотека е необходимо да обработва описаните по-долу категории с лични данни на потребителите на библиотеката.

(1) Категории лични данни и цели на обработването

- ✓Физическа идентичност : Име, ЕГН, Адрес, Паспортни данни (без копия на документи по ЗБДС/, Месторождение, Телефон, Имейл адрес.
- ✓Социална идентичност : Образование, Трудова дейност, Пол (мъж, жена)
- ✓Семейна идентичност : Родствени връзки

(2) Основания за обработване

Личните данни се предоставят на АЛД или от съответните лица, за които те се отнасят или от Директора на Библиотеката във всички случаи, когато е необходимо и след получаване на изрично и информирано съгласие от лицето, за което се отнасят личните данни. Когато не е налице хипотезата на чл. 4, ал. 1, т.1 от Закона за защита на личните данни, физическите лица, чиито данни се обработват от Библиотеката, подписват декларация по образец (**Приложение №1**). Законовите основания за обработване на данните са посочени в Закона за обществените библиотеки, Правилника за дейността на Библиотеката, Стандарта за библиотечно-информационно обслужване, Закона за счетоводството и др. , и имат за цел да се улеснят административните функции и оперирането на информационните технологии, за администриране на съществуващи и бъдещи договорености, и за предоставяне на продукти и услуги, както и да се осигури съответствие със законовите изисквания, права и задължения, извършване на одити, съобразяване с изискванията на различните власти, ако е необходимо да се отговаря в случай на съдебен процес като призовки, търсене на законови права и средства за защита, защита при спорове, управление или претенции и в съответствие с вътрешните политики и процедури. Заемането на библиотечни единици, само по себе си, е договор. В този смисъл, като изискуем реквизит, за да бъде договорът валиден, са личните данни на лицето.

(3) Лица, на които данните могат да бъдат разкривани:

- ✓физическите лица, за които се отнасят данните;
- ✓на трети лица, по силата на договор;
- ✓на лица, обработващи личните данни;
- ✓на предвидени в закон държавни органи.

(4) Технология на събиране и обработване

Цитираните лични данни по чл. 3, ал. 1. се събират чрез попълване на данните от личната карта на читателя.

(5) Събираните лични данни по ал. 1 са необходими за издаване на читателски карти, за водене на статистика и за защита на фондовете на Регионална библиотека „Ем. Попдимитров“ Кюстендил от недобросъвестно поведение от страна на читателите.

(6) Данните се предоставят доброволно от читателя на длъжностното лице на гише „Регистрация“ за издаване на карта, позволяваща достъп до услуги в Регионална библиотека „ Ем. Попдимитров“.

(7) Библиотеката като АЛД, събира лични данни директно от потребителите, съгласно чл. 19 от ЗЗЛД и задължително информира физическото лице за необходимостта от набиране на лични данни, категориите лични данни и целите, за които ще бъдат използвани личните данни, получателите или категориите получатели, на които личните данни могат да бъдат разкрити, задължения или доброволен характер на предоставянето на лични данни и последствията от тяхното непредоставяне, както и правото на достъп до личните данни и правото на поправката им, ако са неточни. Ако е приложимо, на лицето се предоставя и останалата информация, предвидена в чл. 20 от ЗЗЛД.

(8) При необходимост от поправка или актуализиране на личните данни, лицето предоставя такива на длъжностното лице, определено със заповед на Директора.

(9) Личните данни от Регистър „Потребители“ се съхраняват на хартиен, технически и/или електронен носител в предвидените в нормативен акт срокове. След изтичане на установения срок те се унищожават по заповед на Директора на Библиотеката, като за изпълнението се съставя налдежен протокол.

(10) Пренос на личните данни от Регистъра „Потребители“ по електронен път се извършва при осигуряване на необходимото ниво на защита в съответствие с действащото законодателство с цел осъществяване на законовите задължения на Библиотеката.

(11) Библиотеката може да предоставя личните данни от Регистъра „Потребители“ на трети лица, обработващи личните данни от името на Директора в съответствие с определените в тази Инструкция цели и ред и при осигуряване на необходимата защита.

(12) Защитата на личните данни в Регистър „Потребители“ се осигурява чрез предвидените мерки в тази Инструкция.

.....

IV. ТЕХНОЛОГИЧНО ОПИСАНИЕ НА ВОДЕНЕТО НА РЕГИСТРИТЕ

Чл. 7. Носители на данни

Директорът може да съхранява категориите лични данни, съдържащи се в регистрите на хартиени и/или технически и/или електронни носители при спазване на приложимото законодателство и необходимите мерки за защита.

(1) Срок на съхранение

Личните данни в Регистрите се съхраняват за период, необходим за изпълнение на правните и бизнес нужди на Библиотеката и във връзка с изпълнение на дейностите й по закон, в зависимост от съответния регистър, категорията лични данни и целите за обработката им. Личните данни няма да се съхраняват по-дълго, отколкото е необходимо за защита на законните интереси на АЛД или за счетоводни цели, или в съответствие с изискванията на приложимите закони. Данните, обработвани от Регионална библиотека „Ем. Попдимитров“, ще бъдат унищожени след изтичане периода на пазене, в съответствие с изискванията, наложени в тази Инструкция.

Сроковете за съхранение по отделните регистри са както следва :

РЕГИСТЪР „Потребители“- 6 години

(2) Определяне на длъжностите, свързани с обработване и защита на лични данни, правата и задълженията им.

Длъжностите, свързани с обработване и защита на лични данни, правата и задълженията им, определени в тази точка, са приложими за всички Регистри, изброени в настоящата Инструкция.

Лицето по защита на лични данни е директорът или упълномощено от него лице, което отговаря за контрола върху достъпа и използването на личните данни.

Директорът или упълномощеното от него лице имат следните правомощия :

- Осигурява организацията по водене на регистрите, съгласно предвидените мерки за гарантиране на адекватна защита;
- Следи за спазването на конкретните мерки за защита и контрол на достъпа, съобразно спецификата, оценката на въздействието и нивото на защита на водените регистри;
- Осъществява контрол по спазване на изискванията за защита на регистрите;
- Поддържа връзка с Комисията за защита на личните данни относно предприетите мерки и средства за защита на регистрите и подадените заявления за предоставяне на лични данни.

- Специфицира техническите ресурси, прилагани за обработка на личните данни;
- Следи за спазването на организационните процедури за обработване на личните данни и за спазване на контролирания достъп до носителите на лични данни;
- Провежда периодичен контрол за спазване на изискванията по защита на данните и при открити нередности взема мерки за тяхното отстраняване;

Достъп до личните данни, съхранявани в Регистрите, имат само служители на Регионална библиотека „Ем. Попдимитров“, на които такъв им е необходим за изпълнение на служебните им задължения, както и за изпълнение на бизнес цели, при стриктно спазване на принципа „Необходимост да се знае“ (т.е. в съответствие с правата и задълженията му по длъжностна характеристика и/или договор за съответното правоотношение с Директора). По-конкретно тези служители са „Човешки ресурси”, „Счетоводство”, както и други лица, упълномощени при изпълнение на дейности по длъжностна характеристика или за изпълнение на конкретно възложена задача на принципа „Необходимост да се знае“. Възможността за достъп до личните данни при обработката им на други служители в библиотеката е ограничена до случаите, когато на тях изрично е предоставено такова право на достъп и в съответствие с принципа „Необходимост да се знае“. Правото на достъп се предоставя за всеки конкретен случай от структурата, в който е включен служителят, на когото се дава достъп, с изрично разрешение, в което се посочват личните данни и целите, за които се предоставя достъпът, както и времето, за което се предоставя.
Личните данни, обработвани от Библиотеката, са защитени от разкриване на трети лица. Трети лица не могат да имат достъп до такава информация, освен ако не съществува „Необходимост да се знае“ за такъв достъп. Разкриване на такава информация трябва да бъде изрично разрешено от Директора, като се предприемат подходящи мерки, които да осигурят спазването на законодателството в областта на личните данни, както и спазването на задължението за конфиденциалност (което се налага, чрез изискване от третата страна да подпише споразумение за поверителност) и обезопасяване предаването на всякакъв обмен на данни.
Настоящата инструкция е задължителна за всички служители на АЛД, доколкото те участват в обработването на личните данни по регистрите, и други лица, които имат постоянен или временен достъп до лични данни от всички регистри.

Тези служители, както и други лица, на които е възложено обработването на лични данни от Регистъра, са длъжни :

- Да обработват личните данни законосъобразно и добросъвестно;
- Да използват личните данни, до които имат достъп, съобразно целите, за които се събират и да не ги обработват допълнително по начин, несъвместим с тези цели;
- Да актуализират регистрите с личните данни (по необходимост);
- Да заличават или коригират личните данни, когато се установи, че са неточни или непропорционални по отношение на целите, за които се обработват;
- Да поддържат личните данни във вид, който позволява идентифициране на съответните физически лица за период не по-дълъг от необходимия за целите, за които тези данни се обработват;

- Да спазва тази Инструкция, както и другите вътрешни правила.

V. ВИДОВЕ ЗАЩИТА, ТЕХНИЧЕСКИ И ОРГАНИЗАЦИОННИ МЕРКИ

Чл. 8. Физическа защита на личните данни, съдържащи се в Регистрите

(1) **Организационни мерки** :

- Определяне на зони с контролиран достъп;
- Всички физически зони с хартиени и електронни записи се съхраняват и са ограничени само за служители, които трябва да имат достъп чрез принципа „Необходимост да се знае“ с оглед изпълнението на работните им задължения.
- Всички записи и документи на хартиен носител, съдържащи лични данни, са в заключени шкафове, които са с ограничен достъп, достъпен само за упълномощен персонал.
- Определяне на помещенията, в които ще се обработват лични данни. Личните данни се обработват в непубличната част от помещенията, която е физически ограничена и достъпна само от служители, за които е необходимо да имат достъп с оглед на изпълнение на служебните им задължения.

(2) **Технически мерки**:

- Ключалки
- Шкафове
- Оборудване на помещения
- Пожарогасителни средства

Чл. 9. Персонална защита

Познаване на нормативната уредба в областта на защитата на лични данни се разглежда в обучителната програма, която трябва да бъде премината от служителите при наемането им на работа. Тренировка на персонала за реакция при събития, застрашаващи сигурността на данните се предоставя в обучителна програма. Служителите са обучени незабавно да уведомят прекия си ръководител, ако имат съмнение или е известна заплаха за сигурността.

Чл. 10. Документална защита

(1) Определяне на регистрите, които ще се поддържат на хартиен носител;

(2) Определяне на условията за обработване на лични данни

Личните данни се събират само с конкретна цел, за да подкрепят законните интереси на администратора на лични данни или, доколкото е необходимо, да се съобразят със законовите задължения на администратора на лични данни. Всеки тип данни се класифицира в съответствие с неговото предназначение и характер и са защитени в съответствие с изискванията, посочени по-горе.

(3) Регламентиране на достъпа до регистрите

Достъпът до регистрите е ограничен и се предоставя само на упълномощения персонал от отдел „Човешки ресурси“ или от счетоводния отдел, в съответствие с принципа „Необходимост да знае“.

1. Контрол на достъпа до регистрите

Ръководителите на Счетоводството са отговорни за контрола на достъп до регистрите.

2. Правила за размножаване и разпространение на лични данни

Личните данни могат да бъдат копирани и разпространявани само от „Счетоводство” или от „Човешки ресурси“, ако е необходимо за юридически нужди, както и да бъдат предоставяни на лица, на които са необходими във връзка с извършване на възложена работа. Неразрешеното копиране и разпространение е обект на официални санкции, в зависимост от тежестта на престъплението, включително прекратяване на трудовите взаимоотношения.

3. Процедури за унищожаване

Документите на хартиен носител, които съдържат лични данни, трябва да бъдат унищожени по сигурен начин, когато вече не са необходими за дейностите на библиотеката или правни цели чрез шредиране. Всеки служител и ръководител на структурно звено, който е в притежание на такива документи, е отговорен за сигурното унищожаване на документите. Счетоводителят е отговорен за осигуряването на съответствие с изискванията за сигурно унищожаване. За всяко унищожаване се издава нарочна заповед на директора на библиотеката и съставяне на последващ налдежен протокол.

Чл. 11. Защита на автоматизираните информационни системи и/или мрежи

(1) Идентификация и автентификация

- ✓ Потребителски акаунти и пароли - с цел да се въведе достъп, съобразен с принципа „Необходимост да се знае“, библиотеката изисква мулти потребителските информационни системи да прилагат уникални потребителски акаунти и лични пароли за всеки потребител с акаунт за достъп до мрежата.
- ✓ Отговорност на целия персонал - членовете на персонала са лично отговорни за правилното използване на техните потребителски акаунти и пароли.
- ✓ Създаване на потребителски акаунт - всеки от мрежовите потребителски акаунти на член от екипа следва да бъде поискан от ръководителя на екипа.

(2) Защита от вируси

Библиотеката създава и поддържа стандартни и сигурни конфигурации за всяка компютърна и мрежова платформа, с която оперира. Системният софтуер се контролира и поддържа от оторизирани лица. Сканиране на компютърни вируси – хардуерът на библиотеката трябва да работи и да бъде актуализиран с версии на одобрен антивирусен софтуер скрининг и вирусните подписи на компютрите да бъдат активирани.

(3) Поддържане/експлоатация

Оценка на сигурността и тестване - Библиотеката периодично ще провежда оценки на сигурността, уязвимостта и тестове за проникване в системи и мрежи, за сигурността на информацията и/или неприкосновеността на личните данни.

(4) Копия/резервни копия за възстановяване

Архивиране на информацията - Информацията, съдържаща лични данни трябва да бъде архивирана в съответствие със стандартите за архивиране на данни. Ако бъде необходимо, трябва да се инсталира или предостави техническа помощ за резервен хардуер. Всички архиви, съдържащи данни за производство и/или поверителна информация, трябва да се съхранява с физически контрол на достъпа и трябва да се инвентаризира регулярно.

(5) Криптографска защита

Криптирането се използва за защита на личните данни, които се предават от АЛД по електронен път или за преносими носители, когато такива данни се предават извън логическия или физически контрол на АЛД.

(6) Процедури по унищожаване

След постигане целта на обработване на личните данни или преди прехвърлянето на контрола върху обработването, личните данни, съдържащи се в Регистрите следва да бъдат унищожени или прехвърлени на друг администратор на лични данни, съобразно изискванията на Закона за защита на личните данни при спазване на долупосочените процедури.

Личните данни, съхранявани на електронен носител и сървъри трябва да бъдат унищожени чрез трайно изтриване, като презаписване на електронните средства или физическо унищожаване на средствата или сървъра. Лицето, което отговаря за този процес, е Директорът/или негов пълномощник. Трета страна, ангажирана въз основа на сключен договор да провежда безопасни процеси по унищожаването от името на администратора, е длъжна да предостави Протокол за извършено унищожаване на лични данни.

VI. САНКЦИИ И ОТГОВОРНОСТ ПРИ НАРУШАВАНЕ НА ПРАВИЛАТА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

1. Всяко умишлено нарушение на правилата и ограниченията за достъп до личните данни от служителите на библиотеката може да бъде основание за налагане на дисциплинарни санкции, включително и уволнение. Известни или предполагаеми нарушения трябва да бъдат разследвани от „Човешки ресурси“ и/ или ръководителя на съответния служител.
2. Освен оповестените изисквания от Закона, всички трети лица, обработващи данните, които имат достъп до лични данни, се изисква да подпишат споразумение за обработка на данни и да спазват строги задължения за поверителност.
3. Право на достъп на лицата, чиито лични данни се обработват.

Всяко физическо лице има право на достъп до отнасящи се за него лични данни. Правото на достъп се осъществява с писмено заявление до директора **(Приложение 2).** Заявлението може да бъде отправено и по електронен път по реда на Закона за електронния документ и електронния подпис (ЗЕДЕП). Заявлението се отправя лично от физическото лице или от изрично упълномощено от него лице чрез нотариално заверено пълномощно.

Директорът отказва достъп до лични данни, когато те не съществуват или предоставянето им е забранено със закон.

В случаите, когато при осъществяване правото на достъп на физическото лице, могат да бъдат разкрити лични данни и за трето лице, Директорът е длъжен да предостави на съответното физическо лице достъп до частта от тях, отнасяща се само за него.

VI. ПРЕДОСТАВЯНЕ НА ЛИЧНИ ДАННИ В ТРЕТИ СТРАНИ

Лични данни от Регистрите могат да бъдат предоставяни в страни извън Европейския съюз само след спазване на законовите изисквания и получаване на необходимите разрешения от КЗЛД.

VII. ДОПЪЛНИТЕЛНИ РАЗПОРЕДБИ

По смисъла на настоящата инструкция:

1. Администратор на лични данни е Регионална библиотека „Ем. Попдимитров” Кюстендил, със седалище и адрес на управление гр. Кюстендил, ул. „Л. Каравелов” 1.
2. Лице по защита на личните данни е физическо лице, притежаващо необходимата компетентност, директорът на Регионална библиотека „Ем. Попдимитров“ или друго лице, което е назначено или упълномощено от Директора със съответен писмен акт, в който са уредени правата и задълженията му във връзка с осигуряването на необходимите технически и организационни мерки за защита на личните данни при тяхното обработване.
3. Обработващ личните данни е физическо или юридическо лице, държавен орган или орган на местното самоуправление, който обработва лични данни от името на Администратора на лични данни.
4. Лице с достъп до данни е всяко лице, действащо под ръководството на директора или на обработващия, което има достъп до лични данни, може да ги обработва само по указание на Директора, освен ако в закон е предвидено друго.
5. Обработване на лични данни е всяко действие или съвкупност от действия, които могат да се извършват по отношение на личните данни с автоматични или други средства, като

събиране, записване, организиране, съхраняване, адаптиране или изменение, възстановяване, консултиране, употреба, разкриване чрез предаване, разпространяване, предоставяне, актуализиране или комбиниране, блокиране, заличаване или унищожаване.

6. Регистър на лични данни е всяка структурирана съвкупност от лични данни, достъпна по определени критерии, централизирана, децентрализирана или разпределена на функционален или географски принцип.
7. Наредбата е Наредба №1 от 30. 01. 2013г. за минимално ниво на технически и организационни мерки и допустимия вид защита на личните данни.

IX.ПРЕХОДНИ И ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

2. По отношение на обработването и защитата на личните данни, всички вътрешни процедури от документооборота на Регионална библиотека „Ем. Попдимитров“ трябва да бъдат в съответствие с разпоредбите на ЗЗЛД и настоящата инструкция.

3. Инструкцията е задължителна за всички служители и други лица, наети на граждански договор от библиотеката, и са длъжни да я спазват.

4. Контрол по изпълнението на настоящата инструкция се осъществява от Директора на библиотеката и/или упълномощени от него длъжностни лица.

5. Изменения и допълнения на тази инструкция се правят по реда на издаването и утвърждаването и.

ДИРЕКТОР: С. Пейчева