

ПРАВИЛА

**за защита сигурността на личните данни, задължителни за служителите в
Регионална Библиотека „Любен Каравелов” - Русе,
оторизирани с достъп до регистри с лични данни**

Утвърдил:	Директор:	Теодора Евтимова	
Дата на последна промяна:	Март 2022 г.		

съгласно чл. 3, ал. 3 от Наредба № 1 за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни

I. ОБЩИ ПОЛОЖЕНИЯ

Чл.1(1) Регионална библиотека „Любен Каравелов“/наричана за краткост „Библиотеката“ или „Библиотека“/ с ЕИК по Булстат 000523666 и адрес: гр. Русе 7000 ул. „ Дондуков-Корсаков” № 1 е „администратор на лични данни“ по отношение на събиране и обработване на лични данни, което е необходимо за изпълнение на функциите на културния институт.

(2) Регионална библиотека „Любен Каравелов“ обработва данни в качеството на администратор, вписан в Регистъра на администраторите на лични данни и на водените от тях регистри, поддържан от Комисията за защита на личните данни /КЗЛД/ с идентификационен номер 154895, регистрационен номер 94634.

Чл.2.(1).В качеството си на публичен орган Библиотеката има длъжностно лице по защита на личните данни

(2) Длъжностното лице по защита на личните данни изпълнява най-малко следните задачи:

а) информира и съветва служителите на библиотеката за задълженията, свързани със събирането и обработването на лични данни, по силата на Общия регламент относно защитата на данните и на други разпоредби за защитата на данни на равнище Европейски съюз или държава членка и съгласно Закона за защита на личните данни и настоящите Вътрешни правила

б) наблюдава спазването на законодателството в областта защита на личните данни и настоящите Вътрешни правила по отношение на защитата на личните данни, включително възлагането на отговорности, повишаването на осведомеността и обучението на персонала, участващ в операциите по събирането и обработката на лични данни и съответните одити.

в) при поискване предоставя съвети по отношение на оценката на въздействието върху защитата на личните данни и наблюдава оценяването

г) сътрудничи си с Комисията за защита на личните данни в качеството ѝ на надзорен орган на Република България по всички въпроси, предвидени в Общия регламент относно защитата на данните или произтичащи от други правни актове на Европейския съюз или от законодателството на Република България или по въпроси, инициирани от надзорния орган

д) консултира физически лица във връзка със събирането и обработването на лични данни

от библиотеката, приема и обработва постъпили искания за упражняване на права в съответствие с чл. 30 от Общия регламент относно защитата на данните, води регистър на дейностите по обработване на лични данни в Регионална библиотека „Любен Каравелов”

е) води регистър за нарушенията на сигурността на данните

ж) води регистър за искания от субекти на данни

(3) Данните за контакт с длъжностното лице по защита на личните данни се обявяват на леснодостъпно място на електронната страница на Регионална библиотека „Любен Каравелов” и се съобщават на Комисията за защита на личните данни съгласно чл. 37, пар. 7 от Регламент (ЕС) 2016/679.

(4) Длъжностно лице по защита на личните данни се определя от Директора на Регионална библиотека „Любен Каравелов”.

Предмет

Чл. 3. (1) Настоящите правила за защита на личните данни/наричани за краткост „вътрешни правила“ или „правилата“/ определят условията и реда за събиране и обработване на лични данни, актуализация, съхранение, предоставяне, трансфер, унищожаване, водене на регистри на лични данни, минималното ниво на технически и организационни мерки за тяхната защита в Регионална библиотека „Любен Каравелов“.

(2) Правилата са изготвени в съответствие с изискванията на Регламент (ЕС) 2016/679 на Европейския Парламент обнародван в Официален вестник на Европейския съюз от 04.05.2016 г. и със Закона за защита на личните данни

(3) Правилата се утвърждават, допълват, изменят и отменят от Директора на Регионална библиотека „Любен Каравелов“-Русе

(4) Правилата са предназначени за всички служители в библиотеката, които в рамките на изпълнение на служебните си задължения обработват данни

4. Чл. Настоящите Правила уреждат:

1. Достъп до лични данни и задължения на лицата, които обработват лични данни.
2. Принципите, процедурите и механизмите за обработка на личните данни.
3. Процедурите за уведомяване на надзорния орган в случай на нарушения в сигурността.
4. Процедурите за администриране на искания за достъп до данни, коригиране на обработваните данни, възражения и оттегляне на съгласия, както и администриране на искания за упражняване на други права, които субектите на лични данни имат по закон.
5. Правилата за предаване на лични данни на трети лица в България и чужбина.
6. Необходимите технически и организационни мерки за защита на личните данни от неправомерно обработване и в случай на инциденти, като случайно или незаконно унищожаване, загуба, неправомерен достъп, изменение или разпространение.
7. Техническите ресурси, прилагани при обработката на лични данни.
8. Видовете регистри, които се водят в Регионална библиотека „Любен Каравелов“.

II. ДЕФИНИЦИИ

Чл. 5. За целите на настоящите правила, използваните понятия имат следното значение:
Лични данни – всяка информация, свързана с идентифицирано физическо лице или физическо

лице, което може да бъде идентифицирано („субект на данни“); физическо лице, което може да бъде идентифицирано, е лице, което може да бъде идентифицирано, пряко или непряко, по-специално чрез идентификатор като име, идентификационен номер, данни за местонахождение, онлайн идентификатор или по един или повече признаци, специфични за физическата, физиологичната, генетичната, психическата, умствената, икономическата, културната или социална идентичност на това физическо лице.

Обработване на данни – всяка дейност, която е свързана с използването на лични данни. Това включва: получаване, записване, съхранение, извършване на операция или серия от операции с данните като напр. организиране, редактиране, възстановяване, използване, предоставяне, изтриване или унищожаване. Обработването също включва и трансфер на лични данни до трети лица.

Администратор на лични данни – физическо или юридическо лице, публичен орган, агенция или друга структура, която сама или съвместно с други определя целите и средствата за обработването на лични данни.

Длъжностно лице по защита на данните – физическо лице или организация, определени съгласно изискванията на чл. 37 и сл. от ОРЗД.

Известия по защита на данните – отделни известия, съдържащи информация, предоставяна на субектите на данни в момента, в който Институтцията събира информация за тях. Тези известия могат да бъдат както общи (напр. адресирани към работници и служители или известия на уебсайта на организацията), така и отнасящи се до обработване със специфична цел.

Получател – физическо или юридическо лице, публичен орган, агенция или друга структура, пред която се разкриват личните данни, независимо дали е трета страна или не.

Трета страна – физическо или юридическо лице, публичен орган, агенция или друг орган, различен от субекта на данните, администратора, обработващия лични данни и лицата, които под прякото ръководство на администратора или обработващия лични данни имат право да обработват личните данни.

Съгласие – всяко свободно изразено, конкретно, информирано и недвусмислено указание за волята на субекта на данни, посредством изявление или ясно потвърждаващо действие, което изразява съгласие за обработка на лични данни, свързани с него.

III. ЦЕЛИ И ПРИНЦИПИ НА ОБРАБОТВАНЕ НА ЛИЧНИТЕ ДАННИ

Чл. 6. Настоящите правила се приемат с цел да регламентират:

1. Процедури и механизми за гарантиране защита на личните данни.

2. Необходимите технически и организационни мерки за защита на личните данни от Правата и задълженията на длъжностните лица, обработващи лични данни и/или лицата, които имат достъп до лични данни и работят под ръководството на обработващите лични данни, тяхната отговорност при изпълнение на тези задължения.

3. Правата и задълженията на длъжностните лица, обработващи лични данни и/или лицата, които имат достъп до лични данни и работят под ръководството на обработващите лични данни, тяхната отговорност при изпълнение на тези задължения.

4. Процедури за докладване, управляване и реагиране при инциденти.

Чл. 7. Принципи за защита на личните данни:

1. Законосъобразност, добросъвестност и прозрачност - обработване при наличие на законово основание, при полагане на дължимата грижа и при информиране на субекта на данни;

2. Ограничение на целите – събиране на данни за конкретни, изрично указани и легитимни цели и забрана за по-нататъшно обработване по начин, несъвместим с тези цели;

3. Свеждане на данните до минимум – данните да са подходящи, свързани с и ограничени до необходимото във връзка с целите на обработването;

4. Точност – поддържане в актуален вид и предприемане на всички разумни мерки за гарантиране на своевременно изтриване или коригиране на неточни данни, при отчитане на целите на обработването;

5. Ограничение на съхранението – данните да се обработват за период с минимална продължителност съгласно целите. Съхраняване за по-дълги срокове е допустимо за целите на архивирането в обществен интерес, за научни или исторически изследвания или статистически цели, но при условие, че са приложени подходящи технически и организационни мерки;

6. Цялостност и поверителност – обработване по начин, който гарантира подходящо ниво на сигурност на личните данни, като се прилагат подходящи технически или организационни мерки;

7. Отчетност – администраторът носи отговорност и трябва да е в състояние да докаже спазването на всички принципи, свързани с обработването на лични данни.

Чл. 8. Личните данни се обработват законосъобразно, добросъвестно и прозрачно при спазване на гореописаните принципи:

1. Субектът на данните се информира предварително за обработването на неговите лични данни.

2. Личните данни се събират за конкретни, точно определени и законни цели и не се обработват допълнително по начин, несъвместим с тези цели.

1. Личните данни съответстват на целите, за които се събират.

2. Личните данни трябва да са точни и при необходимост да се актуализират.

3. Личните данни се заличават или коригират, когато се установи, че са неточни или не съответстват на целите, за които се обработват.

4. Личните данни се поддържат във вид, който позволява идентифициране на съответните физически лица за период, не по-дълъг от необходимия, за целите, за които тези данни се обработват.

Чл. 9. За да е законосъобразно обработването на данните, трябва да е налице поне едно от следните условия:

1. Субектът на данните е дал своето съгласие.

2. В случаите, когато се обработват лични данни на деца до 14 години, обработването е законосъобразно само ако е дадено съгласие от родител или попечител, чрез попълване на декларация по образец */Приложение 2/*

3. Обработването е необходимо за изпълнението на договор, по който субектът на данните е страна, или за предприемане на стъпки по искане на субекта на данните преди сключването на договор.

4. Обработването е необходимо за спазването на законово задължение, което се прилага спрямо администратора.

5. Обработването е необходимо, за да се защитят жизненоважни интереси на субекта на данните или на друго физическо лице.

6. Обработването е необходимо за изпълнение на задача от обществен интерес.

7. Обработването е необходимо за целите на легитимните интереси на администратора, освен когато пред тези интереси преимущество имат интересите или основните права и свободи на субекта на данни. Целите, за които се обработват лични данни на това основание,

трябва да са описани в приложимите известия по защита на данните.

Чл. 10. Администраторът на лични данни възлага обработването им на негови служители (обработващи) при спазване изискванията на Закона за защита на личните данни.

Чл. 11. Личните данни в Регионална библиотека „Любен Каравелов” се обработват от длъжностни лица, оправомощени от работодателя да отговарят за обработването на лични данни, съгласно § 1, т. 3 от Закона за защита на личните данни.

Чл. 12. Когато не са налице хипотезите на чл. 6, пар. 1, б. „б“ – „е“ от Регламент 2016/679, физическите лица, чиито лични данни се обработват от Регионална библиотека „Любен Каравелов”, подписват декларация за съгласие по образец (*Приложение № 1*).

IV. СУБЕКТИ НА ДАННИ И КАТЕГОРИИ ЛИЧНИ ДАННИ

Чл. 13.(1) Регионална библиотека „Любен Каравелов“ събира и обработва лични данни, необходими за осъществяване на своите права и задължения като работодател, доставчик на услуги и контрагенти при съблюдаване изискванията на приложимото законодателство.

(2) Обработваните лични данни, са групирани в регистри на дейностите по обработване, съдържащи правила за обработване на лични данни, отнасящи се до:

- служители и изпълнители по трудови или граждански договори;
- потребители (читатели);
- доставчици на услуги.
- дарители

(3) Относно лицата, заети по трудови или граждански правоотношения в Библиотеката, и на кандидатите за работа, се събират следните лични данни:

1. Идентификация: име; ЕГН (дата на раждане), постоянен и/или настоящ адрес, телефон, данни по лична карта или паспортни данни, адрес на електронна поща.

2. Образование и професионална квалификация; данни, свързани с образование, трудов опит, професионална и лична квалификация и умения.

3. Здравни данни: здравословно състояние, ТЕЛЖ решения, медицински свидетелства, болнични листове и всяка прилежаща към тях документация.

4. Други данни: свидетелство за съдимост, когато се изисква представянето му съгласно нормативен акт, както и други данни, чието обработване е необходимо за изпълнение на правата и задълженията на Библиотеката като работодател.

5. Относно физически лица, клиенти, потребители, се събират лични данни, които са необходими за изпълнението на законовите задължения на библиотеката като доставчик на услуги, както следва:- име; ЕГН (дата на раждане), постоянен и/или настоящ адрес, телефон, адрес на електронна поща, данни по лична карта или паспортни данни, степен на образование.

6. Относно физически лица, доставчици на услуги на Библиотеката, се съхраняват лични данни, необходими за сключването и изпълнението на договори за предоставяне на услуги на Библиотеката от външни доставчици, както следва:- име, ЕГН (дата на раждане), постоянен и/или настоящ адрес, телефон, данни по лична карта или паспортни данни; адрес на електронна поща.

7. Библиотеката не изисква предоставяне на повече данни от необходимите и нормативно определените.

V. ДОСТЪП ДО ЛИЧНИ ДАННИ

Чл.14. Достъпът до лични данни се осъществява само от лица, чиито служебни задължения или конкретно възложена задача го налагат след запознаване с нормативната уредба в областта

на защитата на личните данни, политиката и ръководствата за защита на личните данни, обработвани от администратора

Чл.15. Всяко лице, чиито служебни задължения налагат събирането, обработката и съхранението на данни преминава през инструктаж, който се удостоверява с Протокол */Приложение 4/* и подписват декларация за неразгласяване на информацията по образец */Приложение 5/*

Чл.16. Достъп до личните данни на работещите имат:

1. Директорът на Регионална библиотека „Любен Каравелов” – Русе – при изпълнение на правомощията му, съгласно Кодекса на труда.

2. Обработващите лични данни – работещите в направление „Финансово-административна и стопанска дейност” при изпълнение на техните задължения, предвидени в съответните нормативни актове, Правилника за дейността на Регионална библиотека „Любен Каравелов” и длъжностните им характеристики.

3. Лицата наети по трудов или граждански договор – всяко от тях само до своите лични данни.

Чл.17. Достъп до личните данни имат библиотекарите, извършващи регистрация и обслужване на читатели в Библиотеката.

Чл.18. Достъп до регистрите, поддържани в Библиотеката, имат и съответните държавни органи, когато са изискали данните по надлежен ред във връзка с изпълнението на техните правомощия и съгласно закона за защита на личните данни.

Чл.19. Обработващите лични данни подписват декларация за спазване на изискванията в настоящите Вътрешни правила */Приложение б/* и тя се прилага в личните им досиета.

Чл.20. Лицата, които работят с лични данни носят отговорност за осигуряване и гарантиране на регламентиран достъп до служебните помещения и опазване на носителите, съдържащи лични данни.

VI. ПРАВА И ЗАДЪЛЖЕНИЯ НА СЛУЖИТЕЛИТЕ

Чл.21. Длъжностните лица обработват личните данни със съгласието на физическото лице.

Чл. 22. Длъжностното лице информира лицето, чиито данни обработва, за:

1. Целта и средствата за обработване на личните данни.
2. Последиците при отказ за предоставяне на лични данни.
3. Правото на достъп до личните данни на лицето.

Чл. 23. Длъжностните лица, обработващи лични данни и такива, имащи достъп до тях, са длъжни:

1. Да предприемат необходимите технически и организационни мерки, за да защитят данните от случайно или незаконно разрушение, случайна загуба или промяна, незаконно разкриване или достъп, нерегламентирано изменение или разпространение, както и от всички други форми на обработване на лични данни.

2. Да сигнализират по етапен ред ръководството на Библиотеката при установени нередности.

3. Да подпишат декларация, в която декларират, че по никакъв начин няма да разпространяват или злоупотребяват с информация за личните данни, до които имат достъп.

Чл. 24. В случай на нарушение на чл. 25-27 лицата носят отговорност по Закона за защита на личните данни.

Чл. 25. За неизпълнение на задълженията от страна на съответните длъжностни лица по настоящите Вътрешни правила и когато неизпълнението на съответното задължение е

констатирано и установено от надлежен орган, се налагат наказания съгласно действащите законови разпоредби на Република България.

ВИ. ВИДОВЕ РЕГИСТРИ, УСЛОВИЯ И РЕД ЗА ВОДЕНЕТО ИМ

Чл.26. Регионална библиотека „Любен Каравелов” поддържа следните видове регистри:

1. Регистър „Потребители” („читатели”)
2. Регистър „Служители и работещи на граждански договор”
3. Регистър „Контрагенти“
4. Регистър „Дарители“

Чл. 27. В регистър „Потребители” („читатели”) се събират и съхраняват лични данни на потребителите (читателите) на Регионална библиотека „Любен Каравелов” с оглед на съхраняване и опазване на библиотечните фондове във връзка с изискванията на Закона за обществените библиотеки, Наредбата за запазване на библиотечните фондове, Закон за задълженията и договорите .

Чл. 28. Групи данни, обработвани в регистър „Потребители” („читатели”):

1. Относно физическата идентичност на лицето: имена; ЕГН; номер, дата и място на издаване на документ за самоличност; адрес
2. Относно образование – образователно-квалификационна степен; специалност.
3. Относно осигуряване средства за комуникация между потребителя и Библиотеката – телефонен номер; електронен адрес.

Чл. 29. (1) Технологичното описание на регистъра обхваща носителите на данни, технологията на обработване, начин на съхраняване и предоставяните услуги по регистъра.

(2) Данните в регистъра се предоставят от физическите лица при регистрацията в Регионална библиотека “Любен Каравелов“

(3) Личните данни се съхраняват в релационна база данни на световен производител – Oracle Corporation. Базата данни е заключена и достъпа до нея се осъществява само чрез средствата за достъп на Библиотечната информационна система (БИС). В БИС се задават права на служителите, които имат достъп до лични данни на потребители (читатели). Достъпът се осъществява от определени служители, съгласно длъжността им, които ползват функциите на БИС за работа с лични данни на потребители (читатели) след легитимация чрез уникално потребителско име и парола. БИС притежава необходимата функционалност за администриране на лични данни.

(4) Данните се съхраняват на специализиран сървър върху защитен дисков масив (по стандарт RAID. Сървърът се намира в заключен комуникационен (сървърен) шкаф в сървърно помещение с ограничен достъп. Достъп до помещението имат само лица от отдел „Автоматизация”. Базата данни (включително личните данни на клиентите) се архивират ежедневно на специализирано устройство за съхранение на данни – NAS (network access storage).

(5) Достъп до сървърното помещение на външни лица (представители на обслужващи фирми или служители) се осъществява само с присъствието на служители от отдел „Автоматизация”. Външните лица могат да имат достъп до технически средства, но не и до информационните ресурси на базата данни или нейните архиви.

(6) Защитата на електронните данни от неправомерен достъп, повреждане, изгубване или унищожаване се осигурява посредством поддържане на антивирусни програми и ежедневно архивиране на данните.

(7) Обработващите лични данни предприемат всички организационно технически мерки за

съхраняването и опазването на личните карти, в това число недопускане на достъпа до тях на външни лица.

(8) Данни не се предоставят на трети лица, освен в случаите, предвидени в законовите разпоредби на Република България.

(9) Водене на хартиен носител се прилага само като временна мярка при възникнали проблеми с електрозахранването или библиотечния софтуер. След отстраняването им всички данни се нанасят в регистъра, а хартиените се унищожават.

(10) Данните в регистъра се съхраняват според Номенклатурата на делата със срокове за съхранение в Регионална библиотека “Любен Каравелов”.

Чл.30. (1) Данните от регистъра се обработват от длъжностни лица от Направление „Обслужване на читатели“, Направление „Ресурсно осигуряване“, Направление „Фондове и каталози“ и Направление „Административно – стопанско“.

(2) Длъжностните лица нямат право да разпространяват информация за личните данни, станали им известни при изпълнение на служебните им задължения.

Чл.31. (1) Най-малко веднъж годишно се извършват периодични проверки за състоянието и целостта на личните данни, съдържащи се в регистъра и относно необходимостта от понататъшното обработване.

(2) Проверката се извършва от комисия назначена със заповед на Директора на Регионална библиотека „Любен Каравелов“.

(3) За работата на комисията по ал. 2 се съставя доклад. Докладът трябва да включва преценка на необходимостта за обработка на личните данни или унищожаване.

(4) За извършеното унищожаване на лични данни и носители на лични данни се съставя Протокол, подписан от служителите по ал. 2, съгласно образец, представляващ *Приложение № 2*

Чл.32. (1) След постигане целта на обработване на личните данни и изтичане на сроковете за съхранение личните данни следва да бъдат унищожени при спазване на процедурите, предвидени в приложимите нормативни актове и в настоящите Вътрешни правила.

(2) В случаите, в които се налага унищожаване на носител на лични данни, Регионална библиотека „Любен Каравелов“ прилага необходимите действия за заличаването на личните данни по начин, изключващ възстановяване данните и злоупотреба с тях, като:

1. Личните данни, съхранявани на електронен носител и сървъри, се унищожават чрез трайно изтриване, вкл. презаписването на електронните средства или физическо унищожаване на носителите.

2. Документите на хартиен носител, съдържащи данни, се унищожават чрез разрязване с помощта на машина – шредер и/или чрез изгаряне нарязване.

Чл.33. (1) При регистриране на неправомерен достъп до информационните масиви за лични данни, или при друг инцидент, нарушаващ сигурността на личните данни, служителят, констатирал това нарушение/инцидент, незабавно докладва за това на прекия си ръководител, който от своя страна е длъжен, своевременно да информира Длъжностното лице по защита на данните за инцидента. Уведомяването за инцидент се извършва писмено, по електронен път или по друг начин, който позволява да се установи извършването му и да се спази изискването за уведомяване на Комисията за защита на личните данни в срок от 72 часа от узнаването за инцидента.

(2) Процесът по докладване и управление на инциденти задължително включва регистрирането на инцидента, времето на установяването му, лицето, което го докладва, лицето, на което е бил докладван, последствията от него и мерките за отстраняването му.

Чл. 34. (1) В регистър „Служители и работещи на граждански договор” се събират и съхраняват лични данни на работещите по трудов или граждански договор в Регионална библиотека „Любен Каравелов”, с оглед:

1. Индивидуализиране на трудовите и граждански правоотношения.
2. Изпълнение на нормативните изисквания на Кодекса на труда, Кодекса за социално осигуряване, Закона за счетоводството, Закона за държавния архив и др.
3. Използване на събраните данни за съответните лица за служебни цели.
4. За всички дейности, свързани със съществуване, изменение и прекратяване на трудовите и граждански правоотношения – за изготвяне на всякакви документи на лицата в тази връзка (договори, допълнителни споразумения, документи, удостоверяващи трудов стаж, служебни бележки, справки, удостоверения и др. подобни).
5. За установяване на връзка с лицето по телефон, за изпращане на кореспонденция, отнасяща се до изпълнение на задълженията му по трудови или граждански договори.
6. За водене на счетоводна отчетност, относно възнагажденията на посочените по-горе лица по трудови и граждански договори.

Чл. 35. Групи данни, обработвани в регистър „Служители и работещи на граждански договор”:

1. Относно физическата идентичност на лицето: имена, ЕГН, адрес, телефон, данни от личната карта.
2. Относно образование – образователно-квалификационна степен, (вид на образованието); специалност; документ за придобито образование; допълнителна квалификация или правоспособност, когато такива се изискват за длъжността, за която лицето кандидатства и др.
3. Относно семейна идентичност на лицата – семейно положение (наличие на брак, развод, брой членове на семейството, в това число деца до 18 години и др.).
4. Относно трудовата дейност – професионална биография, данни от трудовата дейност и др.
5. Относно здравния статус на лицата - карта за предварителен медицински преглед за постъпване на работа.
6. Относно гражданскоправния статус на лицето - свидетелство за съдимост и други документи, удостоверяващи правния статус.

Чл. 36. (1) Технологичното описание на регистъра обхваща формата на носителите на данни, технологията на обработване, срока за съхраняване и предоставяните услуги по регистъра.

(2) Данните в регистъра се обработват на хартиен и технически носител, както следва:

На хартиен носител:

1. Данните се събират в писмена (документална) форма и се съхраняват в трудовото досие (кадрово дело) на всеки работещ в библиотеката или на наетото по граждански договор лице. Кадровите дела се подреждат в специален картотечен шкаф, разположен в Направление „Финансово-административна и стопанска дейност”.
2. Обработващите лични данни предприемат всички организационно технически мерки за съхраняването и опазването на трудовите досиета, в това число недопускане на достъпа до тях на външни лица.
3. Трудовите досиета на работещите или личните на наетите по граждански договор лица не се изнасят извън сградата на администратора на лични данни.
4. Данни от личните досиета не се предоставят на трети лица, освен в случаите,

предвидени в законовите разпоредби на Република България.

5. Длъжностните лица нямат право да разпространяват информация за личните данни, станали им известни при изпълнение на служебните им задължения.

На магнитен и/или оптичен носител:

1. Личните данни се въвеждат в бази данни и на отделни файлове на компютрите на обработващите лични данни

2. Данните се съхраняват на твърд диск, на изолиран компютър. Компютърът е свързан в локална мрежа, но със защитен достъп до личните данни, който е непосредствен само от страна на обработващия лични данни. Софтуерните продукти са адаптирани към специфичните нужди на администратора на лични данни.

3. Непосредствен достъп до компютрите имат само обработващите лични данни.

4. Достъпът до операционната система, съдържаща файлове за обработка на лични данни имат само обработващите лични данни чрез парола, известна само на тях.

5. Компютрите на главния счетоводител и оперативния счетоводител са изолирани в помещения за самостоятелна работа.

6. Защитата на електронните данни от неправомерен достъп, повреждане, изгубване или унищожаване се осигурява посредством поддържане на антивирусни програми и ежедневно архивиране на данните.

7. Длъжностните лица нямат право да разпространяват информация за личните данни, станали им известни при изпълнение на служебните им задължения.

(3) Данните от регистъра се обработват от служители в Направление „Финансово-административна и стопанска дейност”

Чл. 37.(1) Данни от регистъра могат да бъдат предоставяни на държавни институции с оглед изпълнение на нормативно задължение (Националния осигурителен институт, Национална агенция за приходите и др).

(2) Данните от регистъра могат да бъдат предоставяни на определени кредитни институции (банки) във връзка с изплащането на дължимите възнаграждения на физическите лица от този регистър.

(3) Във връзка с използването на куриерски услуги – приемане, пренасяне и доставка и адресиране на пратките до физически лица, могат да бъдат предоставяни необходимите данни за тяхното извършване.

(4) Данните от регистъра се трансферират в други държави единствено при командироване на лицата, като предоставените данни са само за физическата и социалната им идентичност, като се спазват изискванията на глава V на Регламент (ЕС) 2016/679.

Чл. 38. (1) Най-малко веднъж годишно се извършват периодични проверки за състоянието и целостта на личните данни, съдържащи се в регистъра и относно необходимостта от понататъшното обработване.

(2) Проверката се извършва от комисия със заповед на Директора на Регионална библиотека „Любен Каравелов“. Назначена.

(3) За работата на комисията по ал. 2 се съставя доклад. Докладът трябва да включва преценка на необходимостта за обработка на личните данни или унищожаване.

Чл. 39. (1) След изтичане на срока за съхранение на данните, комисия определя кои документи подлежат на унищожение и мястото на извършване на процедурата.

(2) Унищожението се извършва посредством няколко начина, определени в зависимост от наличните към момента на унищожението технически възможности (чрез разрязване с помощта на машина – шредер и/или чрез изгаряне или разрушаване (отваряне) на корпуса на

носителя на данни и др.) или Регионална библиотека „Любен Каравелов“ възлага на изпълнител тези действия с договор с предмет конфиденциално унищожаване на документи.

Чл. 40. В регистър „Контрагенти“ се обработват лични данни на физически лица във връзка с изпълнение на договори, по които Регионална библиотека „Любен Каравелов“ е страна. Същите се обработват с цел:

1. Изпълнение на нормативните изисквания на Закона за съдебната власт, Закон за обществените поръчки, Закон за задълженията и договорите, Търговски закон и др.

2. Управление на човешките ресурси, финансово-счетоводна дейност, осигуряване на материално-техническата база на Библиотеката.

3. За установяване на връзка с лицата.

Чл. 41. Групи данни, обработвани в регистър „Контрагенти“:

1. Физическа идентичност: имена и паспортни данни (ЕГН, номер на лична карта, дата и място на издаване, адрес), телефони за връзка и др.

2. Социална идентичност: данни относно образование, трудова дейност, стаж, професионална биография и др.

3. Лични данни относно съдебното минало на лицата – само в изискуемите от нормативен акт случаи.

Чл. 42. (1) Технологичното описание на регистъра обхваща носителите на данни, технологията на обработване, срока за съхраняване и предоставяните услуги по регистъра.

(2) Данните в регистъра се обработват на хартиен и технически носител.

(3) Личните данни в регистъра се предоставят от физическите лица при встъпване в договорни отношения с Регионална библиотека „Любен Каравелов“.

(4) Данните в регистъра се съхраняват 5 (пет) години след прекратяване на договора и извършен одит. Договорите, сключени в изпълнение на проекти с европейско или международно финансиране, се съхраняват в определения за съответната програма срок.

(5) Администраторът предоставя достъп, справки, извлечения и други данни от съответния регистър, само ако е предвидено в нормативен акт.

Чл. 43. (1) Данните от регистъра се обработват от служители от Направление „Финансово-административна и стопанска дейност“.

(2) Длъжностните лица нямат право да разпространяват информация за личните данни, станали им известни при изпълнение на служебните им задължения.

Чл. 44. (1) Данни от регистъра могат да бъдат предоставяни на държавни институции с оглед изпълнение на нормативно задължение (Националния осигурителен институт, Национална агенция за приходите, Сметна палата и др).

(2) Данните от регистъра могат да бъдат предоставяни на определени кредитни институции (банки) във връзка с изплащането на дължимите възнаграждения на физическите лица от този регистър.

(3) Във връзка с използването на куриерски услуги – приемане, пренасяне и доставка и адресиране на пратките до физически лица, могат да бъдат предоставяни необходимите данни за тяхното извършване.

(4) Данните от регистъра не се трансферират в други държави.

Чл. 45. (1) Най-малко веднъж годишно се извършват периодични проверки за състоянието и целостта на личните данни, съдържащи се в регистъра и относно необходимостта от понататъшното обработване.

(2) Проверката се извършва от служители от Направление „Финансово-административна и стопанска дейност“. Служителят изготвя предложение, което включва преценка на

необходимостта за обработка на личните данни или унищожаване.

Чл. 46. (1) След изтичане на срока за съхранение на данните, комисия определя кои документи подлежат на унищожение и мястото на извършване на процедурата.

(2) Унищожението се извършва посредством няколко начина, определени в зависимост от наличните към момента на унищожението технически възможности (чрез разрязване с помощта на машина – шредер и/или чрез изгаряне или разрушаване (отваряне) на корпуса на носителя на данни и др.) или Висшият съдебен съвет възлага на изпълнител тези действия с договор с предмет конфиденциално унищожаване на документи.

VIII МЕРКИ ЗА ГАРАНТИРАНЕ НИВОТО НА СИГУРНОСТ

Чл.47. Регионална библиотека „Любен Каравелов“ организира и предприема мерки за защита на личните данни от случайно или незаконно унищожаване, от неправилен достъп, от изменение или разпространение, както и от други незаконни форми на обработване на лични данни. Предприеманите мерки са съобразени със съвременните технологични достижения и рисковете, свързани с естеството на данните, които трябва да бъдат защитени.

Чл.48. Регионална библиотека „Любен Каравелов“ прилага адекватна защита на личните данни, която включва:

1. Физическа защита;
2. Персонална защита;
3. Документална защита;
4. Защита на автоматизирани информационни системи и мрежи;
5. Криптографска защита.

Чл.49. Физическата защита на личните данни се осъществява при спазване на следните мерки:

1. В сграда на Регионална библиотека „Любен Каравелов“ са инсталирани: СОТ, пожароизвестителна система, Система за видеонаблюдение.
2. Всички магнитно оптични носители, които се използват за запис на лични данни в резултат на архивиране и изготвяне на копия на базите данни, се съхраняват в метален шкаф.
3. Всички документи на хартиен носител, съдържащи лични данни, се съхраняват в заключени шкафове в кабинетите на упълномощените лица.

Чл. 50. Персоналната защита на личните данни се осъществява при спазване на следните мерки:

1. Лицата, обработващи лични данни, се запознават с Общия регламент за защита на данните, Закона за защита на личните данни, настоящите Вътрешни правила, както и с други нормативни актове, относими към съответната дейност по обработване.
2. Лицата, обработващи лични данни, подписват декларация, с която поемат задължение за неразпространение на лични данни станали им известни във връзка и по време на изпълнение на служебните им задължения. Декларацията се съхранява в кадровото досие на всеки служител.
3. Лицата, обработващи лични данни, се запознават с опасностите за личните данни, обработвани от администратора.

Чл.51. Документалната защита на личните данни се осъществява при спазване на следните мерки:

1. Регистрите с лични данни, обработвани от Регионална библиотека „Любен Каравелов“, се поддържат на хартиен или електронен носител.
2. Обработването на личните данни се извършва в рамките на работното време на

Библиотеката.

3. Достъп до регистрите с лични данни, обработвани от Регионална библиотека „Любен Каравелов“, имат само нейните служители

4. Личните данни се събират само за конкретни цели, в съответствие с нормативните изисквания към Регионална библиотека „Любен Каравелов“.

5. Сроковете за съхранение на личните данни от различните регистри е определен в утвърдената Номенклатура на делата със срокове за съхранение в Регионална библиотека „Любен Каравелов“.

6. Личните данни на хартиен носител се съхраняват в определените за целта служебни помещения в сградата на Регионална библиотека „Любен Каравелов“.

7. Временните документи, копия от документи и работни материали от регистрите, които са на хартиен носител и съдържат лични данни, се унищожават чрез машини за унищожаване на документи (шредер)

8. След изтичане на срока за съхранение документите от регистрите същите се унищожават. Унищожението се извършва посредством няколко начина, определени в зависимост от наличните към момента на унищожението технически възможности (чрез разрязване с помощта на машина – шредер и/или чрез изгаряне или разрушаване (отваряне) на корпуса на носителя на данни и др.) и след подписване на протокол за унищожаване/*Приложение 7/* или Регионална библиотека „Любен Каравелов“ възлага на изпълнител тези действия с договор с предмет конфиденциално унищожаване на документи.

Чл. 52. Защитата на автоматизирани информационни системи и мрежи се осъществява при спазване на следните мерки:

1. При работа с данните от регистрите, поддържани от Регионална библиотека „Любен Каравелов“ 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, съобразно изискванията на БИС за работа с лични данни. За защита на данните е инсталирана антивирусна програма и се извършва периодична профилактика на софтуера и системните файлове.

3. Активирана защитна стена и деинсталирани комуникатори, осигуряващи достъп извън рамките на компютърната мрежа на Регионална библиотека „Любен Каравелов“ и създаващи предпоставка за идентифициране на IP адрес на потребителя и за достъп на злонамерен софтуер и мобилен код за компютрите.

4. Всички магнитно оптични носители, които се използват за запис на лични данни в резултат на архивиране и изготвяне на копия на базите данни, се съхраняват в метален шкаф.

5. Достъпът до компютърната мрежа и до БИС за работа с лични данни се осъществява от длъжностни лица чрез уникално потребителско име и парола (с необходимото ниво на сложност), които се предоставят от сектор „Автоматизация“ в Библиотеката.

Чл. 53. 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.

IX. СРОК НА СЪХРАНЕНИЕ И УНИЩОЖАВАНЕ НА ЛИЧНИ ДАНИИ

Чл.54. В срок до 1 година от отпадане нуждата от съхраняване на събраните лични данни, те се унищожават.

Чл.55. (1) За унищожаване на личните данни се свиква тричленна комисия, съставена от длъжностни лица, отговарящи за събирането и съхраняването на лични данни от съответния регистър. За унищожаването на лични данни се съставя протокол, подписан от членовете на комисията.

(2) Унищожаването на личните данни става чрез изтриване на електронните файлове с информация за лични данни и чрез нарязване на хартиения носител, съдържащ лични данни.

Чл.56. Личните данни на читатели, които не са подновили регистрацията си и не дължат библиотечни документи, не се унищожават.

Чл.57. Личните данни на напуснали служители и на лица, работили по граждански договори, не се унищожават.

Чл.58. Личните данни на дарители на библиотеката не се унищожават в срок до 1 година от отпадане на нуждата за съхранение.

X. ПРАВА НА ФИЗИЧЕСКИТЕ ЛИЦА

Чл.59. (1) Всяко физическо лице, чийто лични данни ще се обработват от администратора, следва да бъде уведомено за:

1. Данните, които идентифицират администратора;
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 надзорен орган – Комисията за защита на личните данни;
9. Източника на данните;
10. Съществуване на автоматизирано вземане на решения, включително профилиране.

(2) 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.

(3) Информацията по ал. 1 се обявява на леснодостъпно място на електронната страница на Регионална библиотека „Любен Каравелов“.

**ХІ. ПРОЦЕДУРИ ЗА ДОКЛАДВАНЕ, УПРАВЛЯВАНЕ И РЕАГИРАНЕ ПРИ
ИНЦИДЕНТИ**

Чл. 60. (1) При регистриране на неправилен достъп/нарушение на сигурността до информационните масиви за лични данни, или при друго нарушение на сигурността на личните данни по смисъла на чл. 4, т. 12 от Регламент (ЕС) 2016/679, служителят, констатирал това нарушение/инцидент, незабавно докладва на прекия си ръководител, който от своя страна е длъжен своевременно да информира длъжностното лице по защита на данните за инцидента.

(2) Уведомяването за инцидент се извършва писмено, по електронен път или по друг начин, който позволява да се установи извършването му.

(3) Длъжностното лице писмено уведомява за инцидента администратора, като му предоставя наличната информация относно характера на инцидента, времето на установяване, вида на щетите, предприетите мерки за ограничаване на щетите.

(4) След уведомяването по ал. 3 администраторът заедно с длъжностното лице по защита на данните предприемат необходимите мерки за предотвратяване или намаляване на последиците от неправилен достъп/нарушението на сигурността, както и възможните мерки за възстановяване на данните.

Чл. 61. (1) В случай че нарушението на сигурността създава вероятност от риск за правата и свободите на физическите лица, чиито данни са засегнати, и след съгласуване с администратора, длъжностното лице по защита на личните данни, организира изпълнението на задължението на администратора за уведомяване на Комисията за защита на личните данни.

(2) Уведомяването на Комисията за защита на личните данни следва да се извърши без ненужно забавяне и когато това е осъществимо не по-късно от 72 часа след първоначалното узнаване на нарушението.

(3) Уведомлението до Комисията за защита на личните данни съдържа следната информация:

1. Описание на нарушението на сигурността, категориите и приблизителният брой на засегнатите субекти на данни и категориите и приблизителното количество на засегнатите записи на лични данни.

2. Името и координатите за връзка на длъжностното лице по защита на личните данни.

3. Описание на евентуалните последици от нарушението на сигурността.

4. Описание на предприетите или предложените мерки за справяне с нарушението на сигурността, включително мерки за намаляване на евентуалните неблагоприятни последици.

(4) Когато има вероятност нарушението на сигурността на личните данни да породи висок риск за правата и свободите на физическите лица, длъжностното лице по защита на личните данни, без ненужно забавяне, уведомява засегнатите физически лица.

Чл. 62. Длъжностното лице по защита на личните данни води регистър за нарушенията на сигурността на данните, който съдържа следната информация:

1. Дата на установяване на нарушението.

2. Описание на нарушението — източник, вид и мащаб на засегнатите данни, причина за нарушението (ако е приложимо).

3. Описание на извършените уведомявания: уведомяване на Комисия за защита на личните данни и засегнатите лица, ако е било извършено.

4. Предприети мерки за предотвратяване и ограничаване на негативни последици за субектите на данни.

5. Предприети мерки за ограничаване на възможността от последващи нарушения на сигурността.

Чл. 63. (1) При възникване и установяване на инцидент се докладва своевременно на служителите в сектор „Автоматизация”, които своевременно информират Директора на Библиотеката.

(2) За инцидентите се води дневник, който се съхранява в сектор Автоматизация. При докладване на инцидент работещите в сектора вписват предполагаемото време или период на възникване, времето на установяване, времето на докладване и името на служителя, установил инцидента.

(3) След анализ от страна на служителите в сектор „Автоматизация” и фирмата, отговаряща за информационната сигурност на Библиотеката, в дневника се записват 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 уведомяване на лицето, отговарящо за защитата на личните данни, като това се отразява в дневника по архивиране и възстановяване на данни.

(5) В случаите на компрометиране на парола тя се подменя с нова, като събитието се отразява в дневника за инциденти.

ХІІ. ОЦЕНКА НА ВЪЗДЕЙСТВИЕТО ВЪРХУ ЗАЩИТАТА НА ДАННИТЕ

Чл.64. Оценката на въздействието е процес за определяне на нивата на въздействие върху конкретно физическо лице или група физически лица в зависимост от характера на обработваните лични данни и засегнатите физически лица при нарушаване на поверителността, цялостността или наличността на личните данни

Чл.65. При оценка на въздействието администраторът отчита характера на обработваните лични данни, както следва:

1. Систематизиране и оценка на лични аспекти, свързани с дадено физическо лице/профилиране/, за анализиране или прогнозиране, по-специално на неговото икономическо положение, местоположение, лични предпочитания, надеждност, поведение и др.

2. Данни, които разкриват расов или етнически произход, политически, религиозни или философски убеждения, членство в политически партии или организации, сдружения с религиозни, философски, политически или синдикални цели, или данни, които се отнасят до здравето, сексуалния живот или човешкия геном

3. Лични данни чрез създаване на видеозапис от видеонаблюдение на публично достъпни райони

4. Лични данни в широкомащабни регистри на лични данни

5. Данни, чието обработване, съгласно решение на Комисията за защита на личните данни, застрашава правата и законните интереси на физическите лица

Чл.66. Оценка на въздействието се извършва за високорискови дейности по обработване и съхранение на лични данни, в случаи на:

1. Първоначалното въвеждане на нови технологии.

2. Автоматизирано обработване, включително профилиране или автоматизирано вземане на решения.

3. Обработване на чувствителни лични данни в голям мащаб.

4. Мащабно, систематично наблюдение на публично обществена зона.

5. Други операции по обработване, съдържащи се в списък на надзорния орган по чл. 35, пар. 4 от Регламент (ЕС) 2016/679.

Чл.67. За формирането на оценката се определят следните нива на въздействие:

1. „**Изключително високо**“ – в случаите, когато неправомерното обработване или съхранение на лични данни би могло да доведе до възникване на значителни вреди или кражба на самоличност, трайни увреждания или смърт на голяма група физически лица

2. „**Високо**“ – в случаите, когато неправомерното обработване или съхранение на лични данни би могло да доведе до възникване на значителни вреди или кражба на самоличност, трайни увреждания или смърт на физическо лице

3. „**Средно**“ – в случаите, когато неправомерното обработване и съхранение на лични данни би могло да създаде опасност от засягане на интереси, разкриващи расов или етнически произход, политически, религиозни или философски убеждения, членство в политически партии или организации, сдружения с религиозни, философски, политически и синдикални цели, здравословно състояние, сексуален живот или човешки геном на отделно физическо лице или група от физически лица

4. „**Ниско**“ – в случаите, когато неправомерното обработване или съхранение на лични данни би застрашило неприкосновеността на личността, личния живот на физическото лице или група физически лица

Чл.68. Длъжностното лице по защита на личните данни извършва оценка на въздействие за всички поддържани регистри

Чл.69. Всеки отделен регистър се оценява по критериите поверителност, цялостност и наличност

Чл.70. Най-високото ниво на въздействие, определено по всеки от критериите в Чл.69 определя нивото на въздействие на съответния регистър

Чл.71. В зависимост от нивото на въздействие се определя и съответното ниво на защита :

1. При ниско ниво на въздействие – ниско ниво на защита

2. При средно ниво на въздействие – средно ниво на защита

3. При високо ниво на въздействие – високо ниво на защита

4. При изключително високо ниво на въздействие – изключително високо ниво на защита

Чл.73. (1) При извършването на оценката на въздействието, при необходимост се иска становище на външни експерти в областта на защитата на личните данни.

(2) При констатирани „изключително високо ниво“ или „високо ниво на въздействие“, при необходимост се извършва консултация с Комисия по защита на личните данни.

ХІІІ ПРЕХОДНИ И ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

Чл.74. За неуредените в настоящите Правила въпроси се прилагат разпоредбите на Закона за защита на личните данни и Правилника за прилагането му.

Чл.75. Настоящите Вътрешни правила се издават в съответствие със Закона за защита на личните данни и съгласно Наредба № 1 за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни.

Чл.76. (1) Правилата за защита сигурността на личните данни в Регионална библиотека “Любен Каравелов“, са приети на Дирекционен съвет (Протокол № 2/08.03.2022г.) и влизат в сила от дата на утвърждаването им със Заповед №9/10.03.2022г.

(2) Вътрешните правила се утвърждават, допълват, изменят и отменят от Директора на Библиотеката.

ПРИЛОЖЕНИЯ

Приложение 1 – Декларация за съгласие от субекта на данните

Приложение 2 – Декларация за съгласие от родител/настойник/попечител

Приложение 3 – Споразумение относно условията за обработване на лични данни

Приложение 4 – Протокол за преминато обучение по защита на личните данни и инструктаж за приложимите в РБ „Любен Каравелов”-Русе

Вътрешни правила относно механизма на обработване на лични данни и тяхната защита

Приложение 5 – Декларация за неразгласяване на лични данни, съхранявани в Регионална библиотека „Любен Каравелов“

Приложение 6 – Декларация за спазване на Вътрешните правила за защита сигурността на личните данни, задължителни за служителите в Регионална Библиотека „Любен Каравелов” - Русе, оторизирани с достъп до регистри с лични данни

Приложение 7 – Протокол за унищожаване на лични данни

Приложение 8 – Оттегляне на съгласие от субекта за обработка на лични данни

Приложение 9 – Уведомление до Националния надзорен орган (Комисията за защита на личните данни) за нарушение на сигурността на личните данни

Приложение 10 – Регистри в Регионална Библиотека „Любен Каравелов” – Русе

Приложение 11 – Регистър за унищожаване на документи в Регионална Библиотека „Любен Каравелов” – Русе