Регионална библиотека „Димитър Талев“ Благоевград
Директор: тел. 0879601178, website: www.libblagoevgrad.org, e-mail: reglibblg.bg

УТВЪРЖДАВАМ:

Дора Ангелова, директор
01 март 2021 г.

ВЪТРЕШНИ ПРАВИЛА

ЗА ЗАЩИТА СИГУРНОСТТА НА ЛИЧНИТЕ ДАННИ, ЗАДЪЛЖИТЕЛНИ ЗА СЛУЖИТЕЛИТЕ В РЕГИОНАЛНА БИБЛИОТЕКА „ДИМИТЪР ТАЛЕВ”, ОТОРИЗИРАНИ С ДОСТЪП ДО РЕГИСТРИ С ЛИЧНИ ДАННИ

БЛАГОЕВГРАД
2021

I. ОБЩИ РАЗПОРЕДБИ

Чл. 1. Тези вътрешни правила уреждат условията и реда за водене на регистри в Регионална библиотека „Димитър Талев” – Благоевград, съгласно Закона за защита на личните данни – 2007 г. и Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни, както и реда за упражняване на контрол при воденето на регистрите по Закона за защита на личните данни.

Чл. 2. (1) Обработване на лични данни е всяко действие или съвкупност от действия, които могат да се извършат 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.

(2) Обработване на личните данни се състои и в осигуряване на достъп до определена информация само за лица, чиито служебни задължения или конкретно възложена задача налага такъв достъп.

Чл. 3. (1) Настоящите правила се приемат с цел да регламентират:

1. Създаване на процедури и механизми за гарантиране на неприкосновеността на личността и личния живот чрез осигуряване на защита на физическите лица при неправомерно обработване на свързаните с тях лични данни в процеса на свободното движение на данните. Определяне на минимална възраст 14 години за изразяване на съгласие от дете при ползване на услугите в Библиотеката.
2. Видовете регистри, които Библиотеката води и поддържа.
3. 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 от всички други форми на обработване на лични данни).
4. 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 неизпълнение на тези задължения.

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

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

2. Определените длъжностни лица по защита на личните данни (ДЛЗЛД) в Регионална библиотека „Димитър Талев” са: главният счетожводител, системният администратор и завеждащ информационно-регистрационен център.

Чл. 3. Настоящите вътрешни правила се прилагат за лични данни по смисъла на Закона за защита на личните данни и се издават на основание чл. 13, ал. 1 от Наредба № 1 за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни на комисията за защита на личните данни.

Чл. 4. Регионална библиотека „Димитър Талев” е администратор на лични данни по смисъла на чл. 3, ал. 1 от Закона за защита на личните данни с идентификационен № 155419 и е регистрирана чрез заявление с електронен подпис с вх. № 101213 / 03.11.2017 в електронния регистър на АЛД до Комисията за защита на личните данни.

Чл. 5. (1) Лични данни са всяка информация, отнасяща се до физическо лице, което е идентифицирано или може да бъде идентифицирано пряко или непряко чрез идентификационен номер или чрез един или повече специфични признаци.

(2) Забранява се обработването на лични данни, разкриващи расов или етнически произход, политически възгледи, религиозни или философски убеждения, както и обработването на генетични данни, биометрични данни за целите единствено на идентифицирането на физическо лице, данни за сексуалния живот или сексуалната ориентация на физическото лице.

(3) Личните данни се събират за конкретни, точно определени и законни цели, обработват се законосъобразно и добросъвестно и не могат да се обработват допълнително по начин, несъвместим с тези цели.

Чл. 6. Принципи за защита на личните данни:

- Законосъобразност, честност и прозрачност – Личните данни трябва да бъдат обработвани по прозрачен начин що се касае до субекта.
- Ограничаване на целта – Архивиране на лични данни, които са в интерес на обществото, няма да се счита за несъвместимо с целите на обработка. Събирането на лични данни трябва да бъде в рамките на необходимото.
- Прецизност - личните данни трябва да са прецизни, точни, пълни и актуални, съобразно целите, за които се събират.
- Съхранение – Личните данни трябва да бъдат съхранявани във формат, в който идентификацията на субекти на данни може да се осъществява за период не по-дълъг от необходимото за целите, за които личните данни са събрани.
- Сигурност и опазване - Личните данни трябва да са защитени с мерки за сигурност, съответстващи на чувствителността на информацията.
- Отчетност – Администраторът на лична информация вече е отговорен и трябва да може да демонстрира спазването на принципите, заложени в регламента.

Чл. 7. Администраторът на лични данни възлага обработването им на негови служители (обработващи), при спазване изискванията на Закона за защита на личните данни.

Чл. 8. Личните данни в Регионална библиотека „Димитър Талев” 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.

II. ВИДОВЕ РЕГИСТРИ В РЕГИОНАЛНА БИБЛИОТЕКА „ДИМИТЪР ТАЛЕВ” – БЛАГОЕВГРАД. УСЛОВИЯ И РЕД ЗА ВОДЕНЕТО ИМ.

Чл. 9. Регионална библиотека „Димитър Талев” поддържа следните видове регистри:

1. Регистър „Ползватели”;

2. Регистър „Персонал”.

Чл. 10. Регистър „Ползватели”:

(1) Регистър „Ползватели” – събира и съхранява лични данни на читателите и потребителите на информация в Регионална библиотека „Димитър Талев” с оглед на съхраняване и опазване на библиотечните фондове.

Чл. 11. Форми на водене на регистъра:

(1) На хартиен носител:

1. Данните се събират в писмена (документална) форма и се съхраняват в читателските картони.

2. Читателските картони се подреждат в специално определени за целта шкафове, които са разположени в обслужващите звена – Заемна за възрастни, Детски отдел, отдел „Изкуство”.

3. Обработващите и операторите на 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.

4. Читателските картони не се изнасят извън сградите на администратора на лични данни.

5. Данни от читателския картони не се предоставят на трети лица, освен в случаите, предвидени в законовите разпоредби на Република България.

(2) На магнитен и/или оптичен носител:

1. Личните данни се въвеждат в бази данни на специализиран приложен софтуер през компютрите на обработващите и операторите на 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 оператора на лични данни. Софтуерните продукти са адаптирани към специфичните нужди на администратора на лични данни.

3. Достъп до електронната база данни, съдържаща файлове за обработка на лични данни, има всеки оператор на лични данни чрез парола за отваряне на тези файлове, известна само на него.

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

Чл. 12. Групи данни, обработвани в **регистър „Ползватели”**:

(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) За учащи се – име на учебното заведение, за работещи – месторабота;

(4) Относно преференциални цени за издаване на читателски карти, на основание чл. 53 от Закона за обществените библиотеки и съгласно Правилата за обслужване на ползвателите в Регионална библиотека „Димитър Талев”: Студентите – студентска книжка със заверка за текущата учебна година; пенсионери с ТЕЛК – решение за ТЕЛК; лица с намалена трудоспособност над 90% или техните лични асистенти – съответното решение на ТЕЛК;

(5) Относно осигуряване средства за комуникация между потребител и Библиотеката – телефонен номер; електронен адрес.

Чл. 13. Регистър „Персонал” – Човешки ресурси:

(1) Събирането и обработката на лични данни се извършва от длъжностното лице: „касиер-домакин”.

(2) Личните данни, събирани в този регистър са:

- име, презиме и фамилия на служителите в Регионална библиотека „Димитър Талев”;
- ЕГН;
- № на лична карта, дата и място на издаване;
- постоянен адрес и пощенски код;
- документ за придобита образователно квалификационна степен, (вид на образованието); специалност; допълнителна квалификация или правоспособност, когато такива се изискват за длъжността, за която лицето кандидатства и др.;
- професионална биография, данни от трудовата дейност, трудова книжка и др.;
- свидетелство за съдимост и други документи, удостоверяващи гражданско- правния статус на лицето;
- карта за предварителен медицински преглед за постъпване на работа;

- семейна идентичност, в това число деца до 18-годишна възраст;
- телефон за връзка;
- имейл адрес.

(3) Данните са необходими за изготвяне на трудови договори, служебни бележки и др. и подаване на информация в НОИ, НАП и обслужващите банки.

(4) Данните се съхраняват в трудовите дела на служителите в хартиен вид. Право на достъп до тези данни имат само „касиер-домакин” и Работодател.

Чл. 14. Регистър „Персонал” – Финансово-стопанска дейност:

(1) Събирането на лични данни се извършва от длъжностните лица: „главен счетоводител”. Личните данни, събирани в този регистър са:

- име, презиме, фамилия на лицето.
- ЕГН;
- № на лична карта, дата и място на издаване;
- постоянен адрес и пощенски код;
- Банкова сметка

(2) Достъп до лични данни в регистър „Персонал” – Финансово-стопанска дейност” имат само определените по длъжностна характеристика длъжностни лица;

(3) Данните, съхранявани в регистър „Заплати и хонорари“ се предоставят само на:

- Физически лица, за които се отнасят данните;
- Съответните ТД на НАП;
- Съответните ТП на НОИ;
- Съответните ТП на ИТ.

(4) Данните се съхраняват на хартиен носител и в електронен вид в отдел „Счетоводство”.

Чл. 15. Групи данни за лица, наети по граждански договор и юридически лица, които са в договорни отношения с Библиотеката, с цел събирането и съхранението на лични данни за горепосочените лица, по време на изпълнение на тези договори, 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 съответната правоспособност, 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 възнагражденията на посочените по-горе лица по трудови и граждански договори.

(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, за допълнителна квалификация или правоспособност, когато такива се изискват за длъжността, за която лицето кандидатства и др.

(3) Относно трудовата дейност – професионална биография, данни от трудовата дейност и др.

(4) Относно гражданско-правния статус на физическите и юридически лица - свидетелство за съдимост и други документи, удостоверяващи правния статус, БУЛСТАТ и ДДС регистрация.

Чл. 16. Форми на водене на регистър „Персонал”:

(1) 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 отдел „Счетоводство”.

2. Обработващите и операторите на 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.

(2) На магнитен и/или оптичен носител:

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

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

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

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

5. Компютърът на главния счетоводител е изолиран в помещение 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.

III. МЕРКИ ЗА ГАРАНТИРАНЕ НИВОТО НА СИГУРНОСТ

Чл. 17. (1) Програмно-апаратни мерки за гарантиране нивото на сигурност:

1. Сървърът за базата данни да е на съвременно техническо ниво.

2. Компютърните работни конфигурации да използват операционна система, съобразно изискванията на приложния софтуер за работа с лични данни.

(2) Минималният набор от системни програмни средства на всяка компютърна конфигурация включва:

1. Съвременна операционна система, съобразена с изискванията на приложния софтуер за работа с лични данни.

2. Антивирусен софтуер за постоянно сканиране.

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

(3) Достъпът до компютърната мрежа и до софтуера за работа с лични данни се осъществява от длъжностни лица със специални кодове, които се предоставят от направление „Проекти, автоматизация, дигитализация” в Библиотеката.

Чл. 18. Физически мерки за гарантиране нивото на сигурност:

(1) Извън рамките на установеното работно време, работните помещения се заключват

(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 огнеупорен и водоустойчив шкаф.

Чл. 19. Организационни мерки за гарантиране нивото на сигурност:

(1) Администраторът изготвя Вътрешни правила за защита сигурността на личните данни, задължителна за служителите в Регионална Библиотека „Димитър Талев” - Благоевград, оторизирани с достъп до регистри с лични данни.

(2) Администраторът осъществява охрана на работните помещения в рамките на видео охраната на двете сгради.

(3) Работните компютърни конфигурации, както и цялата IT инфраструктура, се използват единствено за служебни цели.

(4) Проверката на всички компютърни конфигурации по чл. 5, ал. 1, т. 10 от Наредбата за минималното ниво на техническите и организационни

мерки и допустимия вид защита на личните данни се извършва ежемесечно от системния администратор и системния оператор в Библиотеката.

(5) Обработващите лични данни за различните видове регистри в Библиотеката се определят съгласно задълженията, определени в длъжностната им характеристика.

IV. ДОСТЪП ДО ЛИЧНИ ДАННИ

Чл. 20. Достъпът до личните данни на работещите имат:

1. Директорът на Регионална библиотека „Димитър Талев” – при изпълнение на правомощията му, съгласно Кодекса на труда.

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

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

Чл. 21. Достъп до личните данни в регистър „Ползватели” имат библиотекарите, извършващи регистрация и обслужване на читатели в Библиотеката.

Чл. 22. Архивиране на личните данни на магнитен или оптичен носител се извършва периодично на всеки 30 (тридесет) дни от обработващия лични данни с оглед запазване на информацията за съответните лица в актуален вид.

Чл. 23. Достъп до двата регистъра, 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. 24. ***Операторите на лични данни подписват декларация за спазване на изискванията в настоящите Вътрешни правила и тя се прилага в личните им досиета.***

V. ПРАВА И ЗАДЪЛЖЕНИЯ НА СЛУЖИТЕЛИТЕ

Чл. 25. Длъжностното лице обработва личните данни със съгласието на физическото лице.

Чл. 26. 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. 27. Длъжностните лица, обработващи лични данни и такива, имащи достъп до тях, са длъжни:

1. Да предприемат необходимите технически 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. 28. В случай на нарушение на чл. 25-27 лицата носят отговорност по Закона за защита на личните данни.

VI. ОТГОВОРНОСТИ ПРИ НЕИЗПЪЛНЕНИЕ

Чл. 29. 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.

VII. СРОК НА СЪХРАНЕНИЕ И УНИЩОЖАВАНЕ НА ЛИЧНИ ДАННИ

Чл. 30. В срок до 1 година от отпадане нуждата от съхраняване на събраните лични данни, те се унищожават.

Чл. 31. (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, при спазване разпоредбите на Кодекса на труда, както и 5-годишния давностен срок на Наредба № 3 / 18.11.2014 г. за съхраняването, ползването и разпореждането с документи от библиотечния фонд. За унищожаването на лични данни за определените годишни периоди 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. 32. Личните данни на читатели, които не са подновили регистрацията си 5 години след последната регистрация и не дължат библиотечни документи, се унищожават.

Чл. 33. Личните данни в регистър „Персонал” не се унищожават. Личните данни на напуснали служители и на лица, работили по граждански договори, не се унищожават. Личните данни в регистър „Персонал” се пазят петдесет години, след което се предават в държавния архив, съобразно нормативните изисквания.

VI. ПРОЦЕДУРИ ЗА ДОКЛАДВАНЕ, УПРАВЛЯВАНЕ И РЕАГИРАНЕ ПРИ ИНЦИДЕНТИ

Чл. 34. (1) При възникване и установяване на инцидент се докладва своевременно на лицето, отговорно за защитата на личните данни – системния администратор.

(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, установил инцидента.

(3) След анализ от страна на системния администратор 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 за личните данни, като това се отразява в дневника по архивиране и възстановяване на данни.

(5) В случай на пробив в сигурността на данните, Библиотеката трябва да информира своите субекти на данни в рамките на 72 часа, че е имало такъв пробив.

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

VII. ДОПЪЛНИТЕЛНИ РАЗПОРЕДБИ

По смисъла на тези Вътрешни правила:

§ 1 „Администратор на лични данни” е Регионална библиотека „Димитър Талев” – град Благоевград, ул. „Симеон Велики” № 44, представлявана от Директора на библиотеката.

§ 2. „Обработващ лични данни” са длъжностни лица от Регионална библиотека „Димитър Талев”, с определени по длъжностна характеристика задължения в Библиотеката.

§ 4. Законосъобразното водене на регистрите по ЗЗЛД се организира от главния библиотекар, отговорен служител е „Връзки с обществеността” като длъжностно лице по защита на личните данни и се контролира от Директора на Регионална библиотека „Димитър Талев”.

§ 3. Вътрешните правила влизат в сила от деня на тяхното утвърждаване.

VIII. ПРЕХОДНИ И ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§ 1. За неуредените в настоящите Правила въпроси се прилагат разпоредбите на Закона за защита на личните данни, Правилника за прилагането му и други съотносими нормативни актове.

§ 2. Настоящите Вътрешни правила са изготвени и приети на основание чл. 24, ал. 4 от Закона за защита на личните данни и Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и съгласно Наредба № 1 за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни.

§ 3. Настоящите Вътрешни правила се утвърждават, допълват, изменят и отменят от Директора на Регионална библиотека „Димитър Талев” – Благоевград.

§ 4. Настоящите Вътрешни правила за защита сигурността на личните данни в Регионална библиотека „Димитър Талев“, влизат в сила от датата на утвърждаването им 01.03.2021 г.