РЕПУБЛИКА БЪЛГАРИЯ
РАЙОНЕН СЪД – ПЕТРИЧ

УТВЪРЖДАВАМ:
АТАНАС КОБУРОВ
ПРЕДСЕДАТЕЛ НА РС – ПЕТРИЧ

ВЪТРЕШНИ ПРАВИЛА ЗА МЕРКИТЕ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ В РАЙОНЕН СЪД – ПЕТРИЧ

Чл. 1. Тези Вътрешни правила уреждат условията и реда за водене на регистрите на лични данни, минималното ниво на технически и организационни мерки за тяхната защита, както и контрола при обработването на лични данни в Районен съд – Петрич.

Чл. 2. (1) При обработването на лични данни в Районен съд – Петрич се спазват следните принципи:

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.

(2) Ако конкретната цел или цели, за които се обработват лични данни от РС – Петрич, не изискват или вече не изискват идентифициране

на субекта на данните, РС – Петрич не е задължен да поддържа, да се сдобие или да обработи допълнителна информация, за да идентифицира субекта на данните, с единствена цел да докаже изпълнението на изискванията на Регламент 2016/679.

Чл. 3. (1) Администратор на лични данни е Районен съд – Петрич, със седалище и адрес на управление: гр. Петрич, ул. „Лазар Маджаров" №3.

(2) Личните данни се обработват самостоятелно от РС – Петрич и/или чрез възлагане на обработващ лични данни.

(3) Обработващ лични данни е физическо или юридическо лице, публичен орган или друга структура, която обработва лични данни от името на администратора.

Чл. 4. (1) Личните данни се събират за конкретни, точно определени от закона цели, обработват се законосъобразно и добросъвестно и не могат да се обработват допълнително по начин, несъвместим с тези цели. По-нататъшното обработване на личните данни за целите на архивирането в обществен интерес, за научни, исторически изследвания или за статистически цели не се счита за несъвместимо с първоначалните цели.

(2) Личните данни се съхраняват на хартиен, технически и/или електронен носител, само за времето, необходимо за изпълнение на правомощия, правни задължения на РС – Петрич и/или нормалното му функциониране.

(3) Събирането, обработването и съхраняването на лични данни в регистрите на РС – Петрич се извършва на хартиен, технически и/или електронен носител по централизиран и/или разпределен способ в помещения, съобразно с предвидените мерки за защита и оценката на подходящото ниво на сигурност на съответния регистър.

Чл. 5. (1) Данните в регистрите по чл. 8, ал. 1 се обработват само от съдии и съдебни служители на РС – Петрич, в чиито правомощия по закон, длъжностна характеристика или конкретно възложена задача е определено задължение за обработване на данните от съответния регистър, при спазване на принципа „Необходимост да се знае". Тези лица действат под ръководството и по указания на администратора и са длъжни да познават нормативната уредба в областта на защита на личните данни, тези Вътрешни правила, както и да отчитат рисковете за правата и свободите на физическите лица, чиито лични данни се обработват в РС – Петрич. Лицата под ръководство на администратора подписват декларация или се задължават с длъжностната характеристика да не разгласяват личните данни, до които са получили достъп при изпълнение на задълженията си.

(2) При нарушаване на правилата за достъп до личните данни служителите на РС – Петрич носят дисциплинарна отговорност.

Чл. 6. (1) Всяко физическо лице, чиито лични данни се обработват в РС – Петрич, следва да бъде информирано за:

1. данните, които идентифицират съда;
2. целите и основанието за обработването;

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

4. източника на данните;

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

6. срока за съхранение на данните;

7. правото на достъп, коригиране, изтриване или ограничаване на обработването на събраните данни;

8. правото на жалба до КЗЛД и ИВСС.

(2) Информацията по ал. 1 се публикува на официалната интернет страница на съда.

Чл. 7. (1) Председателя на РС – Петрич определя длъжностно лице по защита на данните, което да отговаря за координиране и прилагане на мерките за защита на личните данни.

(1) За длъжностно лице може да бъде определен служител от РС – Петрич с подходяща квалификация от администрацията на съда.

(2) Длъжностното лице по защита на данните са отчита пряко пред председателя на съда и има следните задължения:

1. да информира и съветва председателя на съда и служителите, които извършват обработване на лични данни, за техните задължения по 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 за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните);

2. при поискване да предоставя съвети по отношение на оценката на въздействието върху защитата на личните данни;

3. да наблюдава спазването на нормативните изисквания в областта на личните данни, включително повишаване на осведомеността и обучението на служителите;

4. да си сътрудничи с ИВСС и КЗЛД;

5. да действа като звено за контакт с КЗЛД и ИВСС и при необходимост да се консултира с комисията, съответно с инспектората по въпросите, свързани с обработването на лични данни.;

6. да води регистъра на дейностите по обработване на личните данни;

Чл. 8. (1) В РС – Петрич се обработват лични данни в следните регистри:

1. Регистър „Страни по граждански дела“;

2. Регистър „Страни по наказателни дела“;

3. Регистър „Страни по изпълнителни дела“;

4. Регистър „Бюро съдимост

5. Регистър „Магистрати“.

6. Регистър „Персонал“;

7. Регистър „Декларации по чл. 343а ЗСВ във вр. с чл. 35 от Закона за противодействие на корупцията и за отнемане на незаконно придобитото имущество“;

8. Регистър „Искания по ЗДОИ“;

9. Регистър „Контрагенти“;

10. Регистър „Видеонаблюдение“.

(2) Общо описание на всеки регистър, категориите лични данни, основанието и целта на обработване, субектите на данните, средствата за обработване, лицата, на които се предоставят и срока за съхраняване се съдържат в регистър на дейностите по обработване на лични данни в Районен съд – Петрич (Приложение №1).

Чл. 9. (1) Районен съд – Петрич осигурява подходящи технически и организационни мерки за защита на личните данни, които се обработват, съобразени с рисковете за правата и свободите на субектите на данните.

(2) При определяне на подходящите мерки за сигурност се вземат предвид рисковете, свързани с обработването като случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или достъп до лични данни.

(3) Мерките могат да включват псевдонимизация на личните данни, способност за гарантиране на постоянна поверителност, цялостност, наличност и устойчивост на системите за обработване, способност за своевременно възстановяване на наличността и достъпа до лични данни в случай на физически или технически инцидент, процес на редовно изпитване, оценка на ефективността на техническите и организационни мерки.

(4) Подходящите технически и организационни мерки се въвеждат към момента на обработването или при въвеждането на нови средства за обработване. Задължението за въвеждане на подходящи мерки се отнася до обема на събраните лични данни, степента на обработването, периода на съхраняването им и тяхната достъпност.

Чл. 10. Видовете защита на личните данни са физическа, персонална, документалнаи и защита на автоматизирани информационни системи и мрежи.

Чл. 11. Физическата защита на личните данни в РС – Петрич се осигурява чрез следните технически и организационни мерки за предотвратяване на нерегламентиран достъп и защита на сградите и помещенията, в които се извършват дейности по обработване на лични данни:

1. личните данни се обработват в служебните помещения на съда на адрес: гр. Петрич, ул. „Лазар Маджаров" №3, достъпът до които е ограничен с пропускателен режим;

2. на входа на сградите се осъществява физическа охрана и видеонаблюдение в цялата сграда;

3. достъпът до 3-ти етаж, се осъществява с устройство (карта/чип) за достъп. Устройствата са поименни и с тях са снабдени само съдиите служителите и охраната на съда;

4. достъпът на външни лица до регистратурата и служба „Деловодство“ се осъществява след проверка на документ за самоличност, а до 3- ти етаж само с придружител от служителите;

5. извън работното време на администрацията, работните помещения и сградата се заключват. Осигурена е охрана със СОТ.

6. помещенията, в които се обработват лични данни са оборудвани с пожароизвестителна система и пожарогасителни уреди;

7. всички документи на хартиен носител, съдържащи лични данни, се съхраняват единствено в работните помещения на съдиите, служителите и архива на съда.

Чл. 12. Персоналната защита на личните данни се осъществява при спазване на следните мерки:

1. достъпът до лични данни се осъществява от лица, чиито служебни задължения или конкретно възложена задача налагат такъв достъп, при спазване на принципа „Необходимост да се знае";

2. всички служители са длъжни да спазват нормативната уредба за защита на личните данни, тези правила, всички допълнителни мерки и указания на администратора, както и да познават рисковете за личните данни, обработвани в съда;

3. лицата, обработващи лични данни, задължително подписват декларация (Приложение №2) за неразпространение на лични данни, станали им известни във връзка със служебните им задължения. Декларацията се съхранява в кадровото досие на всеки служител. Подписване на декларация не се изисква, ако съответното задължение е включено в длъжностната характеристика на лицето;

4. споделянето на критична информация между служителите (идентификатори, пароли за достъп и др.) е забранено.

Чл. 13. Документалната защита на личните данни в РС – Петрич се осъществява при спазване на следните мерки:

1. документите, съдържащи лични данни, се съхраняват в помещенията на съда;

2. обработването на лични данни на хартиен носител се извършва в работно време и по изключение извън работното време по дежурство;

3. достъп до регистрите имат служителите в съответствие с принципа „Необходимост да се знае";

4. всеки служител е отговорен за контрола на достъпа до документи, съдържащи лични данни, които се обработват в съда;

5. сроковете за съхранение на данните се определят отделно за всяка дейност по обработване;

6. архивирането на документи се осъществява по реда на ПАС;

7. документи, съдържащи лични данни, се унищожават след изтичане на сроковете за съхранението им по начин, непозволяващ тяхното възстановяване;

Чл. 14. Защитата на автоматизираните информационни системи и/или мрежи в Районен съд – Петрич включва следния набор от приложими технически и организационни мерки за предотвратяване на нерегламентиран достъп до системите и/или мрежите, в които се създават, обработват и съхраняват лични данни:

1. електронната обработка се извършва с помощта на специализиран приложен софтуер с необходимите лицензи;

2. служителите, обработващи лични данни, задължително трябва да притежават необходимата компютърна грамотност и умение за работа с използвания софтуер;

3. всеки упълномощен потребител на автоматизираните информационни системи и/или мрежи има личен профил с определени нива на достъп, съобразени с неговите задължения и принципа „Необходимост да се знае";

4. идентификацията и автентификацията на потребителите се реализира със средствата на операционната система и на използваните специализирани софтуерни продукти чрез потребителско име и парола, както и се осъществява достъп до определени продукти чрез оторизация с КЕП;

5. отдалечен достъп се позволява чрез разпореждане на председателя на съда, като в него се упоменава срока, служителя/съдията, часовете за достъп, след което се прекратява;

6. за защита на данните е инсталирана антивирусна програма и се извършва редовно сканиране на компютрите за заплаха от Интернет, външни носители на информация, локалната мрежа;

7. за поддържането на автоматизираните информационни системи и/или мрежи отговаря системния администратор на Районен съд – Петрич, който поддържа базови конфигурации за защита на операционната система, защитни стени, рутери и мрежови устройства. Той следи за своевременно обновяване на системния, технологичния, приложния и антивирусния софтуер;

8. с цел възстановяване на данните от регистрите се поддържат резервни копия за възстановяване на базите данни и на данните във файловата система;

9. сървърното помещение, в което са разположени сървъри и комуникационни средства, от които зависи правилното функциониране на автоматизираните информационни системи и/или мрежи и е подсигурено с допълнително захранване. Помещението е заключено. Достъп до него се осъществява чрез оторизирани лица с карта. Не се допускат външни лица в помещението, а при нужда от чуждо съдействие, не се оставят без надзор.

Чл. 15. (1) Оценка на въздействието се извършва, когато това се изисква съгласно приложимото законодателство и с оглед на риска за физическите лица и естеството на обработка на лични данни, извършвана от съда. Оценка на въздействието се извършва за високорискови дейности по обработване.

(2) Оценка на въздействието е необходима при:

1. първоначално въвеждане на нови технологии;

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

3. обработване на чувствителни лични данни в голям мащаб;

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

(3) Оценката на риска съдържа най-малко:

1. системен опис на предвидените операции по обработване и целите на обработването, включително, ако е приложимо, преследвания от администратора законен интерес;
2. оценка на необходимостта и пропорционалността на операциите по обработване по отношение на целите;
3. оценка на рисковете за правата и свободите на субектите на данни;
4. мерките за справяне с рисковете, включително гаранциите, мерките за сигурност и механизмите за осигуряване на защитата на личните данни и за демонстриране на спазването на настоящия регламент, като се вземат предвид правата и законните интереси на субектите на данни и на други заинтересовани лица.

(4) При извършването на оценката на въздействието се иска становището на длъжностното лице по защита на данните.

(5) Ако извършената оценка на въздействието покаже, че обработването ще породи висок риск, ако администраторът не предприеме мерки за ограничаване на риска, следва да се извърши консултация с Комисията по защита на личните данни преди планираното обработване.

Чл. 17. (1) При регистриране на неправомерен 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 за това на прекия си ръководител, който от своя страна е длъжен 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 и предприетите мерки за ограничаването им.

(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 неправомерния достъп/нарушението на сигурността, както и възможните мерки за възстановяване на данните.

Чл. 18. (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 данните организира изпълнението на задължението на администратора за уведомяване на Комисията за защита на личните данни или ИВСС.

(2) Уведомяването на КЗЛД или ИВСС се извършва без ненужно забавяне и когато това е осъществимо не по-късно от 72 часа след първоначалното узнаване на нарушението.

(3) Уведомлението до КЗЛД или ИВСС съдържа следната информация:

1. описание на нарушението на сигурността, категориите и приблизителния брой на засегнатите субекти на данни и категориите, и приблизителното количество на засегнатите записи на лични данни;

2. името и координатите за връзка с длъжностното лице по защита на личните данни;

3. описание на евентуалните последици от нарушението на сигурността;

4. описание на предприетите или приложените 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 физическите лица.

Чл. 19. (1) В изпълнение на официалните си правомощия или на законоустановени задължения РС – Петрич предоставя лични данни само на държавни органи (НОИ, НАП, МВР, МП, Прокуратурата на РБ, БНБ, и др.), на други институции (търговски банки, Централен депозитар и др.).

(2) В качеството си на работодател РС – Петрич предоставя лични данни на държавни органи и други институции (банки, лечебни заведения и др.) само в случаите, когато това е предвидено в закон.

Чл. 20. (1) С постигане на целта на обработване на личните данни, те се съхраняват в архив за сроковете, определени в номенклатурата на делата със срокове за запазване на отделните видове документи на съда, утвърдена съвместно от председателя на съда и директора на Централен държавен архив.

(2) След изтичане на сроковете за съхранение на данните, комисия назначена от съдия и съдебни служители определя кои документи подлежат на унищожаване. Унищожаването на данните на хартиен или технически носител се извършва по начин, непозволяващ тяхното възстановяване, например чрез разрязване с помощта на машина и/или чрез изгаряне или разрушаване на магнитния носител на данни и др.

Чл. 21. (1) Всяко физическо лице има право на безплатен достъп до обработвани от съда негови лични данни.

(2) Правото на достъп се осъществява с писмено заявление до председателя на съда. Заявлението се подава лично от субекта на данните или от изрично упълномощено лице с пълномощно с нотариална заверка на подписа.

(3) Информацията може да бъде предоставена на субекта или на неговия представител под формата на устна или писмена справка, по електронен път или на технически носител. Информацията се предоставя по посочения от субекта начин, освен в случаите, когато това е забранено от закон.

Чл. 22. (1) Заявленията за предоставяне на достъп до лични данни се разглеждат от длъжностното лице по защита на данните в 30-дневен срок.

(2) Достъпът до лични данни може да бъде ограничен, когато те не съществуват или когато предоставянето им е забранено със закон.

(3) Когато с предоставянето на достъп до лични данни има опасност да се разкрият данни и за трети лица, на субекта се предоставя информация, съдържаща само отнасящи се за него лични данни.

Чл. 23. (1) Всяко физическо лице има право да поиска да заличи или коригира негови лични данни, ако за обработването им не съществува основание или те са непълни, или неточни.

За неуредени в настоящите Вътрешни правила въпроси, са приложими разпоредбите на Общия регламент относно защитата на данните /ЕС/2016/679, приложимото право на ЕС и законодателството на Република България относно защитата на личните данни – Закона за защита на личните данни и нормативните актове, свързани с прилагането му.