ПРОКУРАТУРА НА РЕПУБЛИКА БЪЛГАРИЯ

ГЛАВЕН ПРОКУРОР

ЗАПОВЕД

№ РД-02-13

гр. София, 19.06. 2018 г.

ОТНОСНО: Утвърждаване на Правила за мерките и средствата за защита на личните данни, обработвани в Прокуратурата на Република България

На основание чл. 138, т. 1 от Закона за съдебната власт, чл. 23, ал. 1 от Закона за защита на личните данни и чл. 24, т. 1 от Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27.04.2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни,

ЗАПОВЯДВАМ:

1. Отменям моя Заповед № РД-02-2/28.01.2015 г. за утвърждаване на Инструкция за мерките и средствата за защита на личните данни, обработвани от Прокуратурата на Република България.
2. Утвърждавам Правила за мерките и средствата за защита на личните данни, обработвани в Прокуратурата на Република България.
3. Контрола по изпълнението на правилата по т.2 възлагам на заместника на главния прокурор при ВАП.
4. Правилата по т.2, ведно с настоящата заповед да се публикуват на вътрешноведомствения сайт на прокуратурата.

ГЛАВЕН ПРОКУРОР:

СОТИР ЦАЦАРОВ

София 1000, бул. „Витоша“ № 2, тел: 02/92 19 601, факс: 02/989 01 10, e-mail: office_gp@prb.bg

ПРАВИЛА ЗА МЕРКИТЕ И СРЕДСТВАТА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ, ОБРАБОТВАНИ В ПРОКУРАТУРАТА НА РЕПУБЛИКА БЪЛГАРИЯ

I.ОБЩИ ПОЛОЖЕНИЯ

1.Настоящите правила имат за цел да регламентират механизмите за защита на личните данни, обработвани в ПРБ.

2.В Прокуратурата на Република България се прилагат организационни и технически мерки за защита, които да гарантират нормативно установените принципи на обработване на лични данни - законосъобразност, добросъвестност, прозрачност, ограничение на целите, свеждане на данните до минимум, точност, ограничение на съхранението, цялостност, поверителност и отчетност.

II.АДМИНИСТРАТОР И ОБРАБОТВАЩИ ЛИЧНИ ДАННИ

1.*Администратор на лични данни* е Прокуратурата на Република България - юридическо лице на бюджетно издръжка със седалище София, Булстат: 121817309, адрес: гр. София, бул. „Витоша“ № 2.

2.Структурните звена на ПРБ по чл. 136 от ЗСВ, Бюрото по защита при главния прокурор и учебните и почивни бази - третостепенни разпоредители с бюджет, са *структури с право на достъп до лични данни при администратора-ПРБ*

3.Прокуратурата на Република България обработва личните данни *самостоятелно* или *чрез възлагане на обработващ лични данни.*

4.Административните ръководители в ПРБ, директорите на НСлС и Бюрото по защита и ръководителите на учебни и почивни бази отговарят за прилагането на мерките за защита на личните данни в ръководените от тях структури по т.2.

5.Достъпът и обработването на лични данни се осъществява само от лица, чиито служебни задължения (по длъжностна характеристика) или конкретно възложена задача налагат такъв достъп, при спазване на принципа „*Необходимост да знае*“. Тези лица - магистрати и съдебни служители, действат под ръководството и по указания на администратора и са длъжни да познават и прилагат нормативната областта на защитата на

личните данни, настоящите Правила, както и да отчитат рисковете за правата и свободите на физическите лица, чиито лични данни се обработват в ПРБ. Лицата под ръководството на администратора подписват декларация или се задължават с длъжностната характеристика да не разгласяват личните данни, до които са получили достъп при и по повод изпълнение на задълженията си.
Запознаването с материали по преписки на ПРБ следва да се извършва при спазване на ограниченията, свързани със защитата на лични данни на трети лица.
6.При неспазването на ограниченията за достъп до личните данни и нарушаване на правилата обработване на лични данни магистратите и съдебните служители носят дисциплинарна отговорност.

7.*Обработващ лични данни* е физическо или юридическо лице, публичен орган, агенция или друга структура, която обработва лични данни от името на администратора на лични данни-ПРБ или от името на структурите с право на достъп до лични данни по т. 2.

III.ДЛЪЖНОСТНО ЛИЦЕ ПО ЗАЩИТА НА ДАННИТЕ

1.Длъжностното лице по защита на данните се определя с акт на главния прокурор.

2.За длъжностно лице може да бъде определен прокурор от ВКП/ВАП, следовател от НСлС или съдебен служител от АГП.

3.Данните за контакт с длъжностното лице се публикуват на интернет страницата на ПРБ - www.prb.bg и се съобщават на КЗЛД по образец на уведомление, утвърден от КЗЛД.

4.Длъжностното лице по защита на данните се отчита пряко пред главния прокурор и има следните задължения и отговорности:

4.1. Да предоставя съвети по отношение на оценката на въздействието върху защитата на лични данни;

4.2.Да информира и консултира/съветва администратора на лични данни – главният прокурор и структурите с право на достъп по т.II.2;

4.3. Да наблюдава спазването на нормативните изисквания в областта на личните данни, включително повишаването на осведомеността и

обучението на персонала, както и на служителите от звено "Вътрешен одит";

4.4. Да спазва конфиденциалността на изпълняваните задачи;

4.5.Да си сътрудничи с КЗЛД;

4.6. Да действа като точка за контакт за КЗЛД.

4.7. Да води регистъра на дейностите по обработване на личните данни

IV.РЕГИСТЪР НА ДЕЙНОСТИТЕ ПО ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ

1.ПРБ поддържа в писмена форма, включително в електронен формат, регистър на дейностите по обработване, за които отговаря /Приложение № 1/.

2.Дейности по обработване на лични данни се извършват при осъществяване на правомощията на прокуратурата както и при осъществяване на дейността на администрацията на ПРБ, съгласно Правилника за администрацията на ПРБ.

2.1.***Дейности по обработване при изпълнение на правомощията на прокуратурата*** :

Цели на обработване:

Обработването на лични данни е свързано с изпълнението на правомощията на прокуратурата, изпълнението на нормативно установените функции и задължения на прокурорите и следователите във връзка с дейностите по предотвратяване, разследване, разкриване, наказателно преследване, както и изпълнението на наказанията (ЗСВ, НПК, АПК, ЗИНЗС).

Категории субекти на данни:

Лица по прокурорски преписки, участници в досъдебното и съдебното производство, лица, изтърпяващи наказание.

Категории лични данни:

Данни, свързани с физическата идентичност – име, ЕГН, адрес, данни на лична карта, месторождение, телефон, подпис както и други данни, събирани и съхранявани в хода и за нуждите на разследването.

Категориите получатели, пред които се разкриват личните данни:

Личните данни се разкриват на субектите на данни и лицата, предвидени в нормативен акт.

2.2.Дейности по обработване при осъществяване на функциите на Бюрото по защита при главния прокурор:

Цели на обработване:

Обработването на лични данни е свързано с изпълнението на функциите на Бюрото по защита, съгласно ЗЗЛЗВНП и правилника за неговото прилагане.

Категории субекти на данни:

Лица, застрашени във връзка с наказателно производство, лица, охранявани при условията и по реда на НПК, лица, принудително довеждани до орган на съдебната власт по разпореждане на главния прокурор.

Категории лични данни:

Извън случаите, при които личните данни са класифицирана информация, данни, свързани с физическата идентичност – име, ЕГН, адрес, данни на лична карта, месторождение, телефон, подпис, с физиологичната идентичност – кръвна група, кръвна картина, с психическата и психологическата идентичност – документи относно психическото състояние и здраве, с икономическата идентичност – имотно състояние, финансово състояние, участие или притежание на дялови или ценни книжа в дружества, задължения към трети лица, със социалната идентичност – произход, среда, образование, трудова дейност, със семейната идентичност – семейно положение, родствени връзки, данни, отнасящи се до здравето, както и други данни от справки и отчети от информационни фондове/системи на службите за сигурност и обществения ред

Категориите получатели, пред които се разкриват личните данни:

Личните данни се разкриват на субектите на данни и лицата, предвидени в нормативен акт.

2.3.*Дейности по обработване при осъществяване на дейността на администрацията на ПРБ и другите структури по т. II.2*:

***2.3.1.Дейности по обработване при управлението на човешки ресурси*:**

Цели на обработване:

Лични данни се обработват за индивидуализирането на трудовите, служебните и граждански правоотношения, при спазване на нормативните изисквания - ЗСВ, ПАПРБ, ЗМВР, ЗДСл, КТ, ЗЗД, КСО, ЗСч, ЗДДФЛ, ЗНАФ, НРВПО и др.; за постигане на служебни цели; за внасянето на промени - изменения и прекратяване на трудовите, служебните и гражданските правоотношения с лицата от персонала, за изготвянето на документи във връзка с трудовото правоотношение /допълнителни споразумения, документи удостоверяващи трудов стаж, служебни бележки, справки, удостоверения и др./, за изготвяне на документи, свързани със служебното правоотношение /заповеди за назначаване, преназначаване и прекратяване на служебното правоотношение, за повишаване ранга и/или размера на индивидуалния размер на основната месечна заплата, документи удостоверяващи служебен стаж, служебни бележки, удостоверения, справки за държавните служители и други документи, необходими за представяне пред различни институции, по искане на служител или държавни институции/; за установяване на връзка с лицата от персонала по телефон; за изпращане на кореспонденция във връзка с изпълнение на задължения по сключените със служителите, издаване на служебни карти и др.

Категории субекти на данни:

При управлението на човешки ресурси се обработват лични данни на кандидати за работа и лицата от персонала - прокурори, следователи, съдебни служители, служители по ЗМВР, държавни служители, лица по трудово правоотношение и изпълнители по граждански договори.

Категории лични данни:

Лични данни, свързани с физическата идентичност - име, ЕГН, адрес, данни на лична карта, месторождение, телефон, подпис, с икономическата

идентичност - имотно състояние, имущество и интереси, със социалната идентичност - образование, трудова дейност, данни за здравословното и психическото състояние (медицинско свидетелство, удостоверение за психическо състояние, болнични листове), данни за съдимост (свидетелство за съдимост), лични данни на служителите от БЗ, свързани с гражданството (декларация), образувани досъдебни производства (удостоверения), физическа годност (протокол) и психологична пригодност (заключение), данни относно изучаване на факти и обстоятелства във връзка с кандидатстване за държавна служба (справки), данни, свързани с деклариране на липса на несъвместимост (декларация), данни, свързани със семейно положение, родствени връзки, както и данни, свързани с политически неутралитет (декларация).

Категориите получатели, пред които се разкриват личните данни:

Обработващи лични данни (Служба по трудова медицина), субектите на данни, лица, предвидени в нормативен акт - НАП, НОИ, Инспекция по труда, съдилища, съдебни изпълнители, ВСС, Инспектората към ВСС, НИП и др.

2.3.2.Дейности по обработване при осъществяването на финансово-стопанската дейност:

Цели на обработване:

Лични данни се обработват за изпълнение на задълженията, свързани с воденето на счетоводна отчетност, изплащането на възнагражденията на лицата от персонала, на третите лица-изпълнители по договори за доставка на стоки и услуги, за погасяването на задължения по предявени за плащане изпълнителни листа, изплащане на възнаграждения на вещи лица и др.

Категории субекти на данни:

Лица от персонала – прокурори, следователи, съдебни служители, държавни служители, лица, работещи по трудово правоотношение и изпълнители по граждански договори, трети лица - контрагенти, кредитори, вещи лица, длъжници, участници в наказателното производство.

Категории лични данни:

Лични данни, свързани с физическата идентичност - име, ЕГН, адрес, данни на лична карта, телефон.

Категориите получатели, пред които се разкриват личните данни:

Обработващи лични данни, субектите на данни, лица, предвидени в нормативен акт - НАП, НОИ, Инспекция по труда, ЧСИ, ВСС, АДФИ, Сметната палата и др.

2.3.3.Дейности по обработване по направление правни дейности:

Цели на обработване:

Лични данни се обработват за служебни цели - изготвяне на становища, докладни записки, проекти на документи - решения, писма, съдебни книжа, заповеди, молби и др., при съобразяване с нормативните изисквания по ЗДОИ, ЗЗЛД, ГПК, АПК, КСО, ЗСВ, КТ и др., за установяване на връзка със субекта на данни - изпращане на кореспонденция, за провеждане на процедури по възлагане на обществени поръчки по ЗОП, сключване на договори за доставки и др.

Категории субекти на данни:

Обработват се лични данни на молители, жалбоподатели, заявители, кандидати и участници в процедури за възлагане на обществени поръчки, изпълнители на обществени поръчки, служители.

Категории лични данни:

Лични данни, свързани с физическата идентичност - име, ЕГН, адрес, данни на лична карта, телефон, подпис, лични данни за образование, професионална квалификация.

Категориите получатели, пред които се разкриват личните данни:

Агенция за обществени поръчки, съдебни органи, съдебни изпълнители, участници в процедурите за възлагане на обществени поръчки, обработващи лични данни, субектите на данни, лица, предвидени в нормативен акт и др.

2.3.4.Дейности по обработване, свързани с осъществяването на контролиран достъп до определени места в съдебните сгради или охраната на стопанисвани имоти:

Цели на обработване:

Обработването на лични данни се извършва за целите на осъществяване на контролиран достъп до сгради, помещения и стопанисвани имоти.

Категории субекти на данни:

Служители от персонала на ПРБ, външни лица/посетители, гости, изпълнители по договори, почиващи.

Категории лични данни:

Обработват се образи на лицата, съдържащи се в снимки и видеозаписи.

Категориите получатели, пред които се разкриват личните данни:

Органи на разследване, наблюдавани лица.

***2.3.5.Дейности по обработване на лични данни, свързани с осъществяването на обучителни мероприятия и почивка*:**

Цели на обработване:

Обработването на лични данни се извършва за осигуряване на почивка на магистрати и съдебни служители на ПРБ и членовете на техните семейства и други придружаващи лица, извън членовете на семействата, както и за целите на провежданите обучителни мероприятия.

Категории субекти на данни:

Прокурори, следователи, съдебни служители и членове на техните семейства, преподаватели/обучители, гости.

Категории лични данни:

Лични данни, свързани с физическата идентичност - име, ЕГН, адрес, данни на лична карта, телефон и със семейната идентичност – родствени връзки.

Категориите получатели, пред които се разкриват личните данни:

Общинска администрация.

3.Лични данни се обработват на хартиен и технически носител и се съхраняват в срокове, съгласно действащата в ПРБ номенклатура на делата.

V.ЗАДЪЛЖЕНИЯ НА АДМИНИСТРАТОРА НА ЛИЧНИ ДАННИ:

1.При събиране на лични данни, администраторът на лични данни предоставя чрез структурите с право на достъп по т. II.2 информация на субектите на лични данни следната информация в момента на тяхното получаване:

1.1.Данните, които идентифицират администратора и координатите за връзка с него;

1.2.Координатите за връзка с длъжностното лице по защита на данните;

1.3.Целите на обработването, за което личните данни са предназначени, както и правното основание за обработването им;

1.4. Получателите или категориите получатели на личните данни;

1.5. Срока, за който ще се съхраняват личните данни;

1.6. Правото на субекта на данни да изиска достъп до, коригиране или изтриване на лични данни или ограничаване на обработването на лични данни или правото да се прави възражение срещу обработването, както и правото на преносимост на данните;

1.7.Правото на субекта на данни да подаде жалба до КЗЛД или до съда;

1.8.Дали предоставянето на лични данни е задължително или договорно изискване, или изискване, необходимо за сключване на договор, както и дали субектът на данните е длъжен да предостави личните си данни или да декларира съгласие за обработването им и евентуалните последствия, ако тези данни или декларацията не бъдат предоставени.

Информация се предоставя в обобщена, кратка и разбираема форма на интернет сайта на ПРБ и на структурите по т.II.2.

2.В случай на нарушение на сигурността на личните данни, административните ръководители и ръководителите по т.II.2 са длъжни незабавно след узнаването да уведомят главния прокурор, който е длъжен да уведоми КЗЛД за нарушението на сигурността на личните данни не по-

късно от 72 часа след узнаването, освен ако не съществува вероятност нарушението на сигурността на личните данни да породи риск за правата и свободите на физическите лица.

2.1.Всяко нарушение на сигурността на личните данни се документира в нарочен регистър.

3.Когато нарушението на сигурността на личните данни е вероятно да породи висок риск за правата и свободите на физическите лица, административните ръководители и ръководителите по т.II.2 без ненужно забавяне, съобщават на субекта на данните за нарушението на сигурността на личните данни, освен когато:

- са предприети подходящи мерки за защита и тези мерки са приложени по отношение на личните данни, засегнати от нарушението;

- са взети впоследствие мерки, които гарантират, че вече няма вероятност да се материализира високият риск за правата и свободите на субектите на данни;

- това би довело до непропорционални усилия.

4.Администраторът на лични данни осигурява необходимите финансови, технически и човешки ресурси за определянето и въвеждането на подходящи организационни и технически мерки, съответстващи на рисковете с различна вероятност и тежест за правата и свободите на физическите лица. За определянето на подходящи мерки главният прокурор назначава комисия, в чийто състав задължително участват директорите на дирекции „ИОТ“, „ФСД“ и „АП“ в АГП.

5.Административните ръководители в ПРБ и ръководителите на учебни и почивни бази определят служители в ръководените от тях структури по т.II.2 със следните отговорности:

- извършване на предварителен и последващ контрол на материалите, публикувани в интернет за съответствие с нормативната уредба в областта на защитата на личните данни;

- извършване на преглед и предприемане на действия за актуализиране на договореностите с обработващите лични данни, декларациите, и другите форми на документиране на съгласието на субекта на данни, както и на декларациите и длъжностните характеристики на служителите;

- извършване на периодични проверки за необходимостта от съхраняване на обработваните лични данни;

- изпитване за преценяване на ефективността на прилаганите технически и организационни мерки с оглед гарантиране на сигурността на обработваните лични данни, поне два пъти годишно.

VI.ОЦЕНКА НА ВЪЗДЕЙСТВИЕТО ВЪРХУ ЗАЩИТАТА НА ДАННИТЕ И ПРЕДВАРИТЕЛНИ КОНСУЛТАЦИИ

1.Оценката на въздействието е процес, чиято цел е да опише обработването на личните данни, да оцени неговата необходимост и пропорционалност и да спомогне за управлението на рисковете за правата и свободите на физическите лица, като ги оцени и определи мерки за справяне с тези рискове.

2.Административните ръководители и ръководителите на структурите с право на достъп по т.II.2 дават предложения за извършване на оценка на въздействието по ред, определен от главния прокурор. Оценка на въздействието се извършва:

2.1.когато има вероятност операциите по обработването да доведат до висок риск за правата и свободите на физическите лица;

2.2.при операции на обработване, съгласно оповестения от КЗЛД нарочен списък.

При извършване на оценка на въздействието върху защитата на данните задължително се иска становището на длъжностното лице по защита на личните данни и дирекция „ИОТ“ в АГП.

3.Оценката съдържа най-малко:

3.1.системен опис на операциите по обработване и целите на обработване. Отчита се характера на обработваните лични данни – систематизиране и оценка на лични аспекти, свързани с дадено физическо лице (*профилиране)*; 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 до човешкия геном; лични данни чрез създаване на видеозапис от видеонаблюдение на публично

достъпни райони; лични данни в широкомащабни регистри на лични данни; данни, чието обработване съгласно решение на КЗЛД застрашава правата и законните интереси на физическите лица;

3.2.оценка на необходимостта и пропорционалността на операциите по обработване по отношение на целите;

3.3.оценка на рисковете за правата и свободите на субектите на данни и

3.4. мерките, предвидени за справяне с рисковете.

4.Оценката на въздействието се извършва при възникнала необходимост. Когато има промяна в риска, с който са свързани операциите по обработване, се прави преглед дали обработването е в съответствие с оценката на въздействието.

VII.ТЕХНИЧЕСКИ И ОРГАНИЗАЦИОННИ МЕРКИ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

1.ПРБ като администратор на лични данни осигурява чрез административните ръководители и ръководителите на структурите с право на достъп по т.II.2 подходящи технически и организационни мерки за осигуряване на ниво на сигурност, съобразено с рисковете за правата и свободите на физическите лица.
В структурите по т.II.2 се поддържа актуален списък на обработваните категории лични данни и въведените технически и организационни мерки за защита.

2.При оценката на подходящото ниво на сигурност се вземат предвид преди всичко рисковете, свързани с обработването като случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или достъп до обработвани лични данни.

3.Мерките могат да включват и псевдонимизация и криптиране 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, преценяване и оценка на ефективността на техническите и организационни мерки.

4.Подходящите технически и организационни мерки се въвеждат към момента на определяне на средствата за обработване и към момента на самото 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.

5.С мерките по т.4 администраторът на лични данни гарантира, че по подразбиране се обработват лични данни, които са необходими за всяка конкретна цел на обработването.

6.Когато след извършена оценка на въздействието не е указано друго, в ПРБ се прилагат следните минимални технически и организационни мерки за защита на личните данни:

6.1.Физическа защита:

6.1.1.Зона с контролиран достъп.

- АЛД обработва личните данни в обект на адрес: гр. София, бул. Витоша 2 и на адресите на всички структури по т.II.2.
- Кабинетите са разположени в масивни сгради.
- Входните врати на кабинетите са масивни, със секретна брава.
- В сградите има пропускателен режим.

6.1.2.Личните данни се обработват в кабинетите на определените от ръководителите на структурите по т.II.2 лица.

6.1.3.Елементите на комуникационно-информационните системи (КИС), използвани за обработване на лични данни, се намират в охраняеми зони.

6.1.4.Всички документи на хартиен носител, съдържащи лични данни, се съхраняват в помещения с подходящи мерки за контрол на достъпа до тях само за оправомощени лица.

6.1.5.Помещенията, в които деловодно се обработват лични данни са оборудвани със заключващи се врати, пожароизвестителна система и пожарогасителни средства и при възможност със заключващи се метални шкафове.

6.1.6.Достъп до помещенията, в които се обработват лични данни, имат определените за целта лица. Външни лица се допускат след прилагане на допълнителни мерки за защита на личните данни.

6.1.7.В зоната с контролиран достъп се допускат лица, след проверка на документ за самоличност или служебна карта.

6.2.Персонална защита.

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

6.2.2.Всички служители са длъжни да спазват ограниченията за достъп до личните данни, и са персонално отговорни пред АЛД за нарушаването на принципите за „Поверителност“ и „Цялостност“ на личните данни.

6.2.3.Лицата, обработващи лични данни под ръководството на администратора, при постъпване на работа се запознават с:

- нормативната уредба в областта на защита на личните данни и актовете по нейното прилагане;
- опасностите за личните данни, обработвани от администратора;
- настоящите правила;

- Мерките в конкретната структура по тII.2, предприети за спазване на настоящите правила и всички указания на администратора, които се публикуват на ведомствения информационен сайт на ПРБ .

6.2.4.Най-малко веднъж годишно се провежда обучение, в която програма е включено запознаване с политиката и ръководствата за защита на личните данни, както и документите по т.6.2.3.

6.2.5.Най-малко веднъж годишно се провежда тренировка на персонала за реакция при събития, застрашаващи сигурността на данните.

6.2.6.Лицата, обработващи лични данни под ръководството на администратора, задължително подписват декларация (Приложение № 2), 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. Подписването на декларация не се изисква, ако съответното задължение е включено в длъжностната характеристика на лицето.

6.2.7.Споделяне на критична информация между служителите (като идентификатори, пароли за достъп и т.н.) е забранено.

6.3.Документална защита

6.3.1.Документите, съдържащи лични данни, се съхраняват само в помещения с ограничен достъп.

6.3.2.Обработването на лични данни на хартиен носител се извършва само в работно време, по изключение в извън работно време след разпореждане на административния ръководител.

6.3.3.Достъп до регистрите имат служителите в съответствие с принципа „Необходимост да знае".

6.3.4.Контрол на достъпа до регистрите се упражнява от административния ръководител или определено от него длъжностно лице.

6.3.5.Сроковете за съхранение на данните са определени поотделно за всяка дейност по обработване .

6.3.6.За унищожаване на лични данни административният ръководител назначава комисия;

6.3.7.Документите, съдържащи лични данни се унищожават по начин, непозволяващ тяхното възстановяване.

6.3.8.След унищожаването на документите комисията по т.6.3.6. съставя протокол и го представя на административния ръководител за утвърждаване.

6.3.9.Личните данни могат да бъдат размножавани и разпространявани от упълномощените служители само ако е необходимо за изпълнение на служебни задължения или ако са изискани по надлежния ред от упълномощени лица.

6.4.Защита на автоматизирани информационни системи и/или мрежи (АИС/М).

6.4.1.Личните данни, обработвани в ПРБ, подлежат на електронна обработка.

6.4.2.Електронната обработка се реализира с помощта на специализирани приложни софтуерни продукти и чрез стандартни средства за текстообработка, електронни таблици и др.

6.4.3.При електронната обработка се използват само лицензирани системни и приложни софтуерни продукти или компютърни програми и бази данни, създадени в рамките на трудово правоотношение по реда на Закона за авторското право и сродните му права.

6.4.4.Служителите, обработващи лични данни, задължително трябва да притежават необходимата компютърна грамотност и умение за работа с използваните специализирани софтуерни продукти.

6.4.5.Всеки упълномощен потребител на АИС/М има личен профил с определени нива на достъп, съобразни със неговите задължения и принципа „Необходимост да знае“.

6.4.6.Идентификацията и автентификацията на потребителите се реализира със средствата на операционната система и на използваните специализирани софтуерни продукти чрез потребителско име и парола.

6.4.7.Сроковете за съхранение на данните са определени съобразно съответната дейност по обработване.

6.4.8.Заличаването на личните данните в електронен вид се осъществява чрез стандартните средства на операционната система или със средствата на специализираните софтуерни продукти.

6.4.9.С цел възстановяване на данните от регистрите се подържат резервни копия за възстановяване на базите данни и на данните във файловата система.

6.4.10.Всички външни технически носители, на които се пазят архивни копия на регистрите, се предават от администратора на АИС за съхранение в каса със заключващ механизъм. Право на достъп до архива имат администраторите на АИС и обработващите лични данни.

6.4.11.В помещенията, в които са разположени компютърни и комуникационни средства, е осигурено заключване на помещенията, система за ограничаване на достъпа.

6.4.12.Работните компютърни конфигурации, както и цялата IT инфраструктура, включително и достъпът до интернет, се използват единствено за служебни цели.

6.4.13.Забранено е използването на преносими носители на данни за лични нужди.

6.4.14.Не се разрешава осъществяването на отдалечен достъп до данни от регистрите.

6.4.15.За защита на данните е инсталирана антивирусна програма и се извършва седмична профилактика на софтуера и системните файлове.

6.4.16.За поддържането на АИС/М се определят системни администратори от структурните звена в ПРБ.

6.4.17.Администраторът на АИС/М създава и поддържа базови конфигурации за защита на операционната система, защитни стени, рутери и мрежови устройства. Същият следи за своевременно обновяване (update) на системния, технологичния (офис-пакети и др.), приложния и антивирусния софтуер.

7.Криптографска защита

За криптографска защита се използват стандартните криптографски възможности на операционната система, на системите за управление на бази данни, на комуникационното оборудване, както и квалифицирани електронни подписи (КЕП).

VIII.ДЕЙСТВИЯ ЗА ЗАЩИТА ПРИ АВАРИИ, ПРОИЗШЕСТВИЯ И БЕДСТВИЯ (ПОЖАР, НАВОДНЕНИЕ И ДР.)

1.При възникване и установяване на инцидент, веднага се докладва на административните ръководители и ръководители на структури по т.II.2 и в зависимост от обстоятелства, се уведомяват съответните институции.

2.С наличните ресурси се вземат мерки за ограничаване въздействието върху регистрите, ако това е възможно.

3.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, извършил доклада. След анализ на инцидента, упълномощено лице вписва в дневника 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 разрешение на административните ръководители и ръководители на структури по т.II.2, като това се отразява в дневника по архивиране и възстановяване на данни.

IX.ПРЕДОСТАВЯНЕ НА ЛИЧНИ ДАННИ НА ТРЕТИ ЛИЦА

1. Лични данни, обработвани от администратора, се предоставят на чужди държавни органи единствено в изпълнение на задължения по нормативни актове. При необходимост от такова предоставяне се спазват разпоредбите на Глава шеста от ЗЗЛД.

2.Данни, обработвани при осъществяване на дейност по управление на човешки ресурси, могат да бъдат предоставяни на държавни институции с оглед изпълнение на нормативно задължение *(НОИ, НАП, МВР и др.)*.

3.В качеството си на работодател, в случаите и по ред, предвидени в закон, административните ръководители и ръководители на структури по т.II.2 предоставят лични данни на персонала и на определени кредитни институции *(например банки)*, във връзка с изплащането на дължимите възнаграждения на служители, изпълнители по граждански договори, кредитни задължения и др.

X.РЕД ЗА УНИЩОЖАВАНЕ ИЛИ ЗАЛИЧАВАНЕ НА ЛИЧНИ ДАННИ СЛЕД ПОСТИГАНЕ НА ЦЕЛИТЕ НА ОБРАБОТВАНЕТО

1.При преустановяване на обработването на личните данни в регистрите АЛД е длъжен да ги унищожи, или да ги прехвърли на друг администратор.

2.След изтичане на срока за съхранение на данните, комисия, назначена от административен ръководител/ръководители на структура по т.II.2, определя кои документи подлежат на унищожение, начина и мястото на извършване на процедурата.

2.1.При унищожаването на данните от регистрите се съставя протокол.

2.2. При прехвърлянето на данните от регистрите на друг администратор се оформя двустранен протокол.

3.След постигане целта на обработване на личните данни административен ръководител/ръководители на структура по т.II.2 ги съхранява само в предвидените в закон случаи.

4.АЛД може да възложи на друг АЛД да извърши процедурата по унищожаване на документите по т.2. В писмения акт по възлагането се определят правата и задълженията на изпълнителя във връзка с унищожаване на документите.

5.Унищожаването на данните на хартиен или магнитен носител се извършва по начин, непозволяващ тяхното възстановяване, например чрез разрязване с помощта на машина – шредер и/или чрез изгаряне или разрушаване (отваряне) на корпуса и разтрошаване на носителя на данни и др.

XI.ПРАВО НА ДОСТЪП И ПРАВО НА ИНФОРМАЦИЯ НА ЛИЦАТА, ЧИИТО ЛИЧНИ ДАННИ СЕ ОБРАБОТВАТ

1.Всяко физическо лице има право на безплатен достъп до отнасящи се за него лични данни на основание и по реда на Регламент (ЕС) 2016/679 или на ЗЗЛД в зависимост от целите на обработването.

2.Правото на достъп се осъществява с писмено заявление до Главния прокурор (*Приложение № 3*). Заявлението се подава лично или от изрично упълномощено лице, чрез нотариално заверено пълномощно, което се прилага към заявлението. Заявление може да бъде отправено и чрез административните ръководители/ръководители на структурите по т.II.2, както и по електронен път по реда на Закона за електронния документ и електронните удостоверителни услуги (ЗЕДЕУС).

3.Информацията може да бъде предоставена под формата на устна или писмена справка или на преглед на данните от съответното физическо лице или от изрично упълномощено от него друго лице. Физическото лице може да поиска копие от обработваните лични данни на предпочитан носител или предоставяне по електронен път, освен в случаите, когато това е

забранено от закон. АЛД е длъжен да се съобрази с предпочитаната от заявителя форма на предоставяне на информацията.

4.АЛД разглежда заявлението за предоставяне на пълна или частична информация, и се произнася в съответните срокове, произтичащи от Регламент (ЕС) 2016/679 или ЗЗЛД според целта на обработването.

5.АЛД отказва достъп до лични данни, когато те не съществуват или предоставянето им е забранено със закон или когато са налице други нормативни ограничения.

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

7.Физическото лице има право по всяко време да поиска от АЛД да заличи или коригира негови лични данни, обработването на които не отговарят на изискванията на ЗЗЛД.

8. Когато информацията, съдържа данни, представляващи класифицирана информация, се прилага редът по ЗЗКИ.

Заключителни разпоредби

§1.Контрол по изпълнението на настоящите правила се осъществява от администратора на лични данни.

Приложение № 1

Регистър на дейностите по обработване на лични данни в ПРБ

Приложение № 2

ДЕКЛАРАЦИЯ

Долуподписаният/ата .....,
ЕГН....., Л.К. № ....., издадена на ..... г.

от МВР гр. .....

в качеството си на .....

(длъжност/позиция)

в „.....“,

ДЕКЛАРИРАМ:

1. Запознат/а съм с:

– нормативната уредба в областта на защитата на личните данни;

– политиката и ръководствата за защита на личните данни в .....;

– опасностите за личните данни, обработвани от администратора.

2. Поемам задължения за:

– несподеляне на критична информация между персонала (например идентификатори, пароли за достъп и т.н.);

– неразгласяване на лични данни, до които съм получил/а достъп при и по повод изпълнение на задълженията си, ако това не е предвидено изрично в закон или не застрашава живота и здравето на физическото лице;

Дата:..... **ДЕКЛАРАТОР:**.....

гр./с/ ..... (подпис и фамилия)

Приложение № 3

ДО „.....”

Адрес: .....

З А Я В Л Е Н И Е

ЗА ДОСТЪП ДО ЛИЧНИ ДАННИ

от..... ЕГН .....,
(име, презиме и фамилия)

адрес .....

телефон за контакт .....

Моля, да ми бъде предоставена информация относно личните ми данни, съхранявани в „.....",

а именно:

.....

.....

.....

Желая да получа исканата от мен информация в следната форма:

.....

(необходимото се изписва)

- преглед на информация;
- устна справка;
- писмена справка;
- копия на технически носител;
- по електронен път.

Дата:..... **Подпис:** .....

Администратор на лични данни			
Име и контакти		Длъжностно лице по защита на личните данни	
Име	Прокуратура на Република България	Име	Петър Николов Андреев
Адрес	София, бул. „Витоша“ № 2	Адрес	София, бул. „Витоша“ № 2
Email	prbcont@prb.bg	Email	pandreev@prb.bg
телефон	02/9867671	телефон	02/8036025

Регистър на дейностите по обработване по обработване на лични данни

Дейност на ПРБ	Цел на обработването	Категории субекти	Категории лични данни	Категории получатели	Име на държавата или международната организация в случай на предаване на лични данни	Срокове на изтриване (ако е възможно)	Общо описание на техническите и организационни мерки за сигурност (ако е възможно)	Законово основание за обработка на данните
Дейности, свързани с изпълнението на правомощията по спазване на законността	Обработването на лични данни е свързано с изпълнението на правомощията на прокуратурата, изпълнението на нормативно установените функции и задължения на прокурорите и следователите във връзка с дейностите по предотвратяване, разследване, разкриване, наказателно преследване, както и изпълнението на наказанията	Лица по прокурорски преписки, участници в досъдебното производство, лица, изтърпяващи наказание	Данни, свързани с физическата идентичност – име, ЕГН, адрес, данни на лична карта, месторождение, телефон, подпис както и други данни, събирани и съхранявани в хода и за нуждите на разследването	Личните данни се разкриват на субектите на данни и лицата, предвидени в нормативен акт	Съгласно изискванията на нормативната уредба	Съгласно Номенклатурата на делата в ПРБ	Физическа защита, персонална защита, документална защита, защита на АИС/М, Криптографска защита	ЗСВ, НПК, АПК, ЗИНЗС и др.
Дейности, свързани с осъществяването на функциите на Бюрото по защита при главния прокурор	Обработването на лични данни е свързано с изпълнението на функциите на Бюрото по защита, съгласно ЗЗЛЗВНП и правилника за неговото прилагане.	Лица, застрашени във връзка с наказателно производство, лица, охранявани при условията и по реда на НПК, лица, принудително довеждани до орган на съдебната власт по разпореждане на главния прокурор.	Лични данни, свързани с физическата идентичност - име, ЕГН, адрес, данни на лична карта, месторождение, телефон, подпис, с икономическата идентичност - имотно състояние, имущество и интереси, със социалната идентичност - образование, трудова дейност, данни за здравословното и психическото състояние (медицинско свидетелство, удостоверение за психическо състояние, болнични листове), данни за съдимост (свидетелство за съдимост), лични данни на служителите от БЗ, свързани с гражданството (декларация), образувани досъдебни производства (удостоверения), физическа годност (протокол) и психологична пригодност (заключение), данни относно изучаване на факти и обстоятелства във връзка с кандидатстване за държавна служба (справки), данни, свързани с деклариране на липса на несъвместимост (декларация), данни, свързани със семейно положение, родствени връзки, както и данни, свързани с политически неутралитет (декларация).	Личните данни се разкриват на субектите на данни и лицата, предвидени в нормативен акт	Съгласно чл.26 от ЗЗЛЗВНП: 1.Държави, с които Република България е сключила международни договори, предвиждащи сътрудничество при осъществяване на специална защита; 2. При условията на взаимност.	Съгласно Номенклатурата на делата в ПРБ	Физическа защита, персонална защита, документална защита, защита на АИС/М, Криптографска защита	ЗЗЛЗВНП, ППЗЗЛЗВНП
Дейности на администрацията по обработване на лични данни при управление на човешки ресурси	Лични данни се обработват за индивидуализирането на трудовите, служебните и граждански правоотношения, при спазване на нормативните изисквания - ЗСВ, ПАПРБ, ЗМВР, ЗДСл, КТ, ЗЗД, КСО, ЗСч, ЗДДФЛ, ЗНАФ, НРВПО и др.; за постигане на служебни цели; за внасянето на промени - изменения и прекратяване на трудовите, служебните и гражданските правоотношения с лицата от персонала, за изготвянето на документи във връзка с трудовото правоотношение /допълнителни споразумения, документи удостоверяващи трудов стаж, служебни бележки, справки, удостоверения и др./, за изготвяне на документи, свързани със служебното правоотношение /заповеди за назначаване, преназначаване и прекратяване на служебното правоотношение, за повишаване ранга и/или размера на индивидуалния размер на основната месечна заплата, документи удостоверяващи служебен стаж, служебни бележки, удостоверения, справки за държавните служители и други документи, необходими за представяне пред различни институции, по искане на служител или държавни институции/; за установяване на връзка с лицата от персонала по телефон; за изпращане на кореспонденция във връзка с изпълнение на задълженията по сключените със служителите, издаване на служебни карти и др.	Кандидати за работа и лицата от персонала - прокурори, следователи, съдебни служители, служители по ЗМВР, държавни служители, лица по трудово правоотношение и изпълнители по граждански договори.	Лични данни, свързани с физическата идентичност - име, ЕГН, адрес, данни на лична карта, месторождение, телефон, подпис, с икономическата идентичност - имотно състояние, имущество и интереси, със социалната идентичност - образование, трудова дейност, данни за здравословното и психическото състояние (медицинско свидетелство, удостоверение за психическо състояние, болнични листове), данни за съдимост (свидетелство за съдимост), лични данни на служителите от БЗ, свързани с гражданството (декларация), образувани досъдебни производства (удостоверения), физическа годност (протокол) и психологична пригодност (заключение), данни относно изучаване на факти и обстоятелства във връзка с кандидатстване за държавна служба (справки), данни, свързани с деклариране на липса на несъвместимост (декларация), данни, свързани със семейно положение, родствени връзки, както и данни, свързани с политически неутралитет (декларация).	Обработващи лични данни - Служба по трудова медицина, субектите на данни, лица, предвидени в нормативен акт - НАП, НОИ, Инспекция по труда, съдилища, съдебни изпълнители, ВСС, Инспектората на ВСС, НИП и др.				ЗСВ, ПАПРБ, ЗМВР, ЗДСл, КТ, ЗЗД, КСО, ЗСч, ЗНАФ, НРВПО и др
Дейности на администрацията по обработване на лични данни по направление финансово-стопански дейности	Лични данни се обработват за изпълнение на задълженията, свързани с воденето на счетоводна отчетност, изплащането на възнагражденията на лицата от персонала, на третите лица-изпълнители по договори за доставка на стоки и услуги, за погасяването на задължения по предявени за плащане изпълнителни листа, изплащане на възнаграждения на вещи лица и др.	Лица от персонала – прокурори, следователи, съдебни служители, държавни служители, лица, работещи по трудово правоотношение и изпълнители по граждански договори, трети лица - контрагенти, кредитори, вещи лица, длъжници, участници в наказателното производство.	Лични данни, свързани с физическата идентичност - име, ЕГН, адрес, данни на лична карта, телефон.	Обработващи лични данни, субектите на данни, лица, предвидени в нормативен акт - НАП, НОИ, Инспекция по труда, ЧСИ, ВСС.				ЗСВ, ПАПРБ, ЗМВР, ЗДСл, КТ, ЗЗД, КСО, ЗСч, ЗНАФ, НРВПО и др
Дейности на администрацията по обработване на лични данни по направление правни дейности	Лични данни се обработват за служебни цели - изготвяне на становища, докладни записки, проекти на документи - решения, писма, съдебни книжа, заповеди, молби и др., за установяване на връзка със субекта на данни - изпращане на кореспонденция, за провеждане на процедури по възлагане на обществени поръчки по ЗОП, сключване на договори за доставки и др.	молители, жалбоподатели, заявители, служители, кандидати и участници в процедури за възлагане на обществени поръчки, изпълнители на обществени поръчки	Лични данни, свързани с физическата идентичност - име, ЕГН, адрес, данни на лична карта, телефон, подпис, лични данни за образование, професионална квалификация.	АОП, съдебни органи, съдебни изпълнители, участници в процедурите за възлагане на обществени поръчки, обработващи лични данни, субектите на данни и други лица, предвидени в нормативен акт и др.		Съгласно Номенклатурата на делата в ПРБ	Физическа защита, персонална защита, документална защита, защита на АИС/М, Криптографска защита	при съобразяване с нормативните изисквания по ЗДОИ, ЗЗЛД, ГПК, АПК, КСО, ЗСВ, КТ, ЗОП и др
Дейности по обработване, свързани с осъществяването на контролиран достъп до определени места в съдебните сгради или охраната на стопанисвани имоти	Обработването на лични данни се извършва за целите на осъществяване на контролиран достъп до сгради, помещения и стопанисвани имоти.	Служители от персонала на ПРБ, външни лица/посетители, гости, изпълнители по договори, почиващи.	Обработват се снимки и видеозаписи.	Органи на разследване		три месеца	Физическа защита, персонална защита, документална защита, защита на АИС/М, Криптографска защита	
Дейности по обработване на лични данни, свързани с осъществяването на обучителни мероприятия и почивка	Обработването на лични данни се извършва за осигуряване на почивка на лицата от персонала на ПРБ и членовете на техните семейства, както и за целите на провежданите обучителни мероприятия.	Прокурори, следователи, съдебни служители и членове на техните семейства, преподаватели/обучители, гости.	Лични данни, свързани с физическата идентичност - име, ЕГН, адрес, данни на лична карта, телефон и със семейната идентичност – родствени връзки.	Общинска администрация		Съгласно Номенклатурата на делата в ПРБ	Физическа защита, персонална защита, документална защита, защита на АИС/М, Криптографска защита	