НАЦИОНАЛЕН ИНСТИТУТ НА ПРАВОСЪДИЕТО

София 1000, ул. „Екзарх Йосиф" № 14, тел: 02 9359 100, факс: 02 9359 101
е-поща: nij@nij.bg, уебсайт: www.nij.bg

ВЪТРЕШНИ ПРАВИЛА ЗА МЕРКИТЕ ЗА ЗАЩИТА НА ЛИЧНИ ДАННИ В НАЦИОНАЛНИЯ ИНСТИТУТ НА ПРАВОСЪДИЕТО

(Утвърдени със Заповед № РД-11-81/17.12.2019 г.)

ГЛАВА ПЪРВА ОБЩИ ПОЛОЖЕНИЯ

Чл. 1. Националният институт на правосъдието (НИП) е публична институция и е администратор на лични данни. В изпълнение на изискванията на Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица при обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент) и Закона за защита на личните данни Институтът има задължение да осигури организационна и техническа защита при обработване и съхраняване на лични данни и да гарантира правата на субектите на лични данни, в съответствие с естеството, обхвата и целите на обработването.

Чл. 2. Настоящите Вътрешни правила уреждат условията и реда за обработване на лични данни, водене на регистри на лични данни, минималното ниво на технически и организационни мерки за тяхната защита, разпределението на дейностите и отговорностите на длъжностните лица, обработващи лични данни, мониторинга на дейността по обработването на лични данни в НИП, както и редът за идентифициране на рисковете за правата и свободите на физическите лица и мерките, които се предприемат за тяхната защита.

Чл. 3. При обработването на лични данни в НИП се спазват следните принципи:

1. законосъобразност, добросъвестност и прозрачност – данните се обработват на законово основание, при полагане на дължимата грижа и при информиране на субекта на данни, спазване на етичните норми и забрана за злоупотреба с права;

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 целите, за които се обработват, и ограничени до необходимото за това обработването;

4. точност – поддържане на данните 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 – обработването е по начин, който гарантира подходящо ниво на сигурност на личните данни, като се прилагат подходящи технически или организационни мерки;

7. отчетност – НИП следва да е в състояние да докаже спазването на всички принципи, свързани с обработването на лични данни.

ГЛАВА ВТОРА
ДЕЙСТВИЯ ПРИ ОБРАБОТВАНЕТО НА ЛИЧНИ ДАННИ

Чл. 4. НИП събира, обработва и съхранява лични данни на физически лица за осъществяване на предвидените в Закона за съдебната власт (ЗСВ) основни дейности и функции на Института, свързани с провеждане на обучение и повишаване на професионалната квалификация на съдии, прокурори, следователи, на кандидати за младши съдии, младши прокурори и младши следователи, на съдебни служители, на членовете на Висшия съдебен съвет, главния инпектор и инспекторите от Инспектората на Висшия съдебен съвет, държавни съдебни изпълнители, съдиите по вписванията, съдебните и прокурорските помощници, съдебните заседатели, на инпекторите от Инспектората към министъра на правосъдието и на други служители от Министерство на правосъдието, както и на други лица, когато е предвидено в закон или акт на Министерския съвет.

Чл. 5. (1) За целите на управление на човешките ресурси НИП обработва лични данни на служителите на института, както и на бивши служители и на кандидати за заемане на длъжност в НИП. Данните се обработват на основание предвидените права и задължения на страните по трудово правоотношение в Кодекса на труда и подзаконови нормативни актове, уреждащи трудовите правоотношения. Обработват се данни за идентификация на физическите лица, данни за образование и квалификация, данни за здравето, данни за контакт, както и други данни, изискуеми по силата на специалните закони, които регламентират трудовите правоотношения, данъчно-осигурителните правоотношения, счетоводното отчитане на дейността, безопасните и здравословни условия на труд, както и социалните и икономически въпроси.

(2) Данните по ал. 1 се обрабоват за обучаемите и обучителите в НИП.

Чл. 6. (1) В изпълнение на своите дейности и във връзка с правомощията си НИП обработва лични данни на физически лица при процедури по възлагане на обществени поръчки, при сключване и изпълнение на договорите, в качеството на публичен възложител на обществени поръчки по смисъла на Закона за обществените поръчки (ЗОП) и свързаните с него нормативи актове на националното право и на правото на ЕС.

(2) В зависимост от предмета на обществената поръчка при възлагането, сключването и изпълнението на договорите се обработват лични данни на физически лица относно образователни и професионални данни за лицата, които ще изпълняват поръчката, идентификация и правен статус на лицата, които представляват участника и др. данни, изрично предвидени в ЗОП.

Чл. 7. (1) Националният институт на правосъдието е задължен субект по смисъла на чл. 3, ал. 1 от Закона за достъп до обществената информация (ЗДОИ) за предоставяне на достъп до обществена информация. Във връзка с обработването на исканията по ЗДОИ се обработва информация за отделни субекти на данни, в която може да се съдържат данни за физическа, икономическа, социална или друга идентичност на отделни лица.

(2) При предоставяне на обществена информация НИП не предоставя лични данни на трети лица, освен при тяхното изрично писмено съгласие, или при условията на надделяващ обществен интерес, по реда и условията, предвидени в ЗДОИ.

Чл. 8. В сградата на НИП се извършва видеонаблюдение с охранителна цел. Местата с видеонаблюдение са обозначени. Видеонаблюдението се възлага по договор с външен изпълнител, който обработва данните в качеството си на администратор на лични данник.

Чл. 9. Обработването на лични данни на посетителите на НИП се извършва чрез обработващ лични данни – охранителна фирма, на която е възложена охраната на сградата и която отговаря на изискванията на Закона за частната охранителна дейност. Целта на събирането на лични данни е осигуряване на безопасността на работещите, обучаемите и обучителит в НИП.

Чл. 10. Достъпът до лични данни се осъществява само от лица, чиито служебни задължения или конкретно възложена задача налагат такъв достъп, при спазване на принципа „Необходимост да знае" и след запознаване с нормативната уредба в областта на защитата на личните данни, вътрешните актове и технически и организационни мерки за предотвратяване и/или преодоляване на последствията от настъпили неблагоприятни събития (рискове).

Чл. 11. (1) В качеството си на публичен орган НИП определя длъжностно лице по защита на личните данни.

(2) Длъжностно лице по защита на личните данни се определя от директора на НИП със заповед.

Чл. 12. (1) Длъжностното лице по защита на данните изпълнява най-малко следните задачи:

1. информира и съветва администратора и служителите, които извършват обработване, за техните задължения по силата на Общия регламент относно защитата на данните и на други разпоредби за защитата на данни на равнище Европейски съюз или държава членка;

2. наблюдава спазването на Общия регламент относно защитата на данните и на други разпоредби за защитата на данни на равнище Европейски съюз или държава членка;

3. наблюдава спазването на политиките на администратора по отношение на защитата на личните данни;

4. допринася за повишаване на осведомеността на служителите в НИП, участващи в дейностите по обработване;

5. извършва необходимите одити (проверки) за прилагането на изискванията за защита на личните данни в НИП;

6. при поискване предоставя съвети по отношение на оценката на въздействието върху защитата на данните и да наблюдава нейното извършване;

7. произнася се по постъпили искания за упражняване на права от субекти на данни;

8. 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;

9. действа като точка за контакт за надзорния орган по въпроси, свързани с обработването, включително предварителната консултация, посочена в чл. 36 от Общия регламент относно защитата на данните, и по целесъобразност се консултира по всякакви други въпроси;

10. в съответствие с чл. 30 от Общия регламент относно защитата на данните води регистър на дейностите по обработване на лични данни в НИП;

11. води регистър за нарушенията на сигурността на данните;

12. води регистър за искания от субекти на данни.

(2) Данните за контакт с длъжностното лице по защита на данните се обявяват на леснодостъпно място на сайта на НИП и се съобщават на Комисията за защита на личните данни.

Чл. 13. (1) Всяко физическо лице, чийто лични данни ще се обработват от администратора, може да получи информация 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 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. право 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 в сградата на НИП и на сайта на Националния институт на правосъдието.

ГЛАВА ТРЕТА
РЕГИСТРИ НА ЛИЧНИ ДАННИ

Чл. 14. В НИП се обработват лични данни в следните регистри на дейностите:

1. Регистър „Обучителни дейности“;

2. Регистър „Управление на човешките ресурси“;

3. Регистър „Контрагенти“;

4. Регистър „Достъп до обществена информация“.

Чл. 15. (1) В регистър „Обучителни дейности“ се събират и обработват лични данни на обучаемите и на преподавателите при извършване на обучителните дейности по чл. 249 от Закона за съдебната власт (ЗСВ). Във всички видове и форми на обучение се обработват данни за идентифициране на физическото лице, данни за образование и професионална квалификация и придобити умения, данни за контакт, данни за здравето, както и други данни, изискуеми по силата на специалните закони, които регламентират трудовия и социален статус на магистрати и съдебни служители и на другите лица по чл. 249 ЗСВ, данъчно-осигурителните правоотношения, счетоводното отчитане на дейността.

(2) В регистъра се обработват следните лични данни, в зависимост от групата на участниците в обучителната дейност (магистрати, съдебни служители, кандидати за младши съдии, младши прокурори и младши следователи, други целеви групи, посочени в ЗСВ, както и временни и постоянни преподаватели):

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

2. социална идентичност: данни относно образование (образователна степен и квалификация, допълнителна квалификация и специализация), месторабота, заемана позиция;

3. данни за икономически статус – банкови сметки, осигурителни права и др.;

4. за целите на конкретно обучение се обработват данни за здравословното състояние на лицата;

(3) Регистърът обхваща носителите на данни, технологията на обработване, срока за съхраняване и целевата група. Данните в регистъра се обработват на хартиен и технически (електронен) носител.

(4) Данните в регистъра се предоставят лично от физическите лица, като се съдържат в техни молби, заявления за участие в обучения или заявления за получаване на статут на постоянни или временни преподаватели и др. или в документи, предоставяни от органи на съдебна власт по отношение на обучителите и кандидатите за младши съдии, младши прокурори и младши следователи.

(5) Данните в регистъра се съхраняват както следва: съгласно Вътрешните правила за дейността на учрежденския архив на НИП, утвърдената Номенклатура на делата със сроковете на съхраняване и Наредбата за реда за организирането, обработването, експертизата, съхраняването и използването на документите в учрежденските архиви на държавните и общински институции.

(6) Данните от регистъра се обработват от длъжностни лица от дирекция „Начално и въвеждащо обучение", дирекция „Текущо обучение и международен обмен на магистрати", дирекция "Електронно обучение и информационни ресурси", дирекция „Обучение на съдебната администрация", дирекция „Финанси, бюджет и стопански дейности". Длъжностните лица нямат право да разпространяват информация за личните данни, станали им известни при изпълнение на служебните им задължения.

(7) Данни от регистъра могат да бъдат предоставяни на държавни институции с оглед изпълнение на нормативно задължение (Висшия съдебен съвет, Инспектората към Висшия съдебен съвет, органи на съдебната власт и т.н.), както и на обработващи лични данни, с които администраторът има сключен договор, във връзка с провеждане на обученията.

(8) Данните от регистъра се трансферират в други държави и международни организации единствено при осъществяване на обучителни дейности при спазване на изискванията на Общия регламент.

(9) Най-малко веднъж годишно се извършват периодични проверки за състоянието и целостта на личните данни, съдържащи се в регистъра и относно необходимостта от по-нататъшното обработване.

Чл. 16. (1) В регистър „Управление на човешките ресурси" се обработват лични данни на служители в администрацията на НИП, постоянни и временни преподаватели, кандидати за младши съдии, младши прокурори и младши следователи. Личните данни се обработват с цел:

1. изпълнение на нормативните изисквания на Конституцията на Република България, Закона за съдебната власт, Кодекса на труда, Кодекса за социално осигуряване, Закона за счетоводството, Закона за данъците върху доходите на физическите лица, Закона за задълженията и договорите, Закона за безопасни условия на труд, Наредбата за служебните командировки и специализации в чужбина и др.

2. индивидуализиране на трудовите и граждански правоотношения.

3. използване на събраните данни за съответните лица за служебни цели:

а) за всички дейности, свързани със съществуване, изменение и прекратяване на трудовите и граждански правоотношения;

б) за изготвяне на всякакви документи на лицата в тази връзка (договори, допълнителни споразумения, документи, удостоверяващи трудов стаж, служебни бележки, справки, удостоверения и др. подобни);

в) за установяване на връзка с лицето по телефон, за изпращане на кореспонденция, отнасяща се до изпълнение на задълженията му по трудови или граждански договори;

г) за водене на счетоводна отчетност, удържане на дължими данъци, социални осигуровки и други дейности относно възнагражденията на посочените по-горе лица по трудови правоотношения и граждански договори;

д) за командироване на лицата при изпълнение на служебните им ангажименти.

(2) В регистъра се обработват следните лични данни:

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 (учебно заведение, образователна степен и допълнителна квалификация и специализация), както и трудова дейност, стаж, професионална биография и др.;

3. семейна идентичност: данни относно семейното положение на лицата (наличие на брак, развод, брой членове на семейството, в това число деца до 18 години др.);

4. икономическа идентичност: данни относно имотното и финансово състояние на лицата;

5. лични данни относно съдебното минало на лицата;

6. данни за здравословното и психическото състояния на лицата.

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

(4) Личните данни в регистъра се предоставят от физическите лица при кандидатстване за работа в администрацията на НИП, също и от ВСС за постоянните и временните преподаватели и за кандидатите за младши съдии, младши прокурори и младши следователи. Данните на кандидатите за работа в администрацията на НИП се въвеждат директно в договори, допълнителни споразумения, документи, удостоверяващи трудов стаж, служебни бележки, справки, удостоверения, кореспонденция и др.

(5) Данните в регистъра се съхраняват, както следва: съгласно Вътрешните правила за дейността на учрежденския архив на НИП; съгласно утвърдената Номенклатура на делата със сроковете на съхраняване; съгласно Наредбата за реда за организирането, обработването, експертизата, съхраняването и използването на документите в учрежденските архиви на държавните и общински институции.

(6) Данните от регистъра се обработват от служители от дирекция ФБСД и отдел „Юрисконсулти".

(7) Данни от регистъра могат да бъдат предоставяни на държавни институции с оглед изпълнение на нормативно задължение (Националния осигурителен институт, Национална агенция за приходите, могат да бъдат предоставяни на определени кредитни институции (банки) във връзка с изплащането на дължимите възнаграждения на физическите лица от този регистър.

(8) 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 Общия регламент.

(9) Най-малко веднъж годишно се извършват периодични проверки за състоянието и целостта на личните данни, съдържащи се в регистъра и относно необходимостта от по-нататъшното обработване.

Чл. 17. (1) В регистър „Контрагенти" се обработват лични данни на физически лица във връзка с възлагането и изпълнението на договори, по които НИП е страна. Същите се обработват с цел:

1. изпълнение на нормативните изисквания на Закона за съдебната власт, Закона за обществените поръчки, Закона за задълженията и договорите, Търговския закон и др.;

2. управление на финансово счетоводна дейност, осигуряване на материално-техническата база на НИП и осигуряване на обучителните дейности на НИП;

3. за установяване на връзка с лицата, представители на контрагентите.

(2) В регистъра се обработват следните лични данни:

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.

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

(4) Личните данни в регистъра се предоставят от физическите лица при встъпване в преддоговорни и договорни отношения с НИП.

(5) Данните в регистъра се съхраняват 5 (пет) години след прекратяване на договора и извършен одит от компетентните органи съгласно изискванията на ЗОП. Договорите, сключени в изпълнение на проекти с европейско или международно финансиране, се съхраняват в определения от съответния проект срок.

(6) Данните от регистъра се обработват от служители от дирекция ФБСД и отдел „Юрисконсулти" и от посочените в договора или заповед лица, отговарящи за изпълнението на договора .

(7) Данни от регистъра могат да бъдат предоставяни на държавни институции с оглед изпълнение на нормативно задължение на Националния осигурителен институт, Национална агенция за приходите, Висш съдебен съвет, Прокуратура на Република България, Сметна палата, Агенция за държавна финансова инспекция, Агенция по обществените поръчки и други контролни органи от национално и европейско ниво, на определени кредитни институции (банки) във връзка с изплащането на дължимите възнаграждения на физическите лица от този регистър.

(8) Най-малко веднъж годишно се извършват периодични проверки за състоянието и целостта на личните данни, съдържащи се в регистъра и относно необходимостта от по-нататъшното обработване.

Чл. 18. (1) В регистър „Достъп до обществена информация" се обработват лични данни на физически лица, които сезират НИП с молби, жалби, предложения, заявления за достъп до обществена информация. Същите се обработват с цел:

1. изпълнение на нормативните изисквания на Административнопроцесуалния кодекс, Гражданския процесуален кодекс, Закона за достъп до обществена информация, Закона за защита на личните данни и др.;

2. за установяване на връзка с лицата.

(2) В регистъра се обработват следните лични данни: физическа идентичност - име, адрес, телефон, ЕГН, адрес за кореспонденция, електронна поща и др.

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

(4) Личните данни в регистъра се предоставят от физически лица, за които се отнасят данните, или от други лица в предвидените от нормативен акт случаи, като се съдържат в техните молби, предложения, жалби, заявления и др. или в документи, предоставяни от държавни органи и органи на местното самоуправление, по реда, предвиден в ЗДОИ.

(5) Данните в регистъра се съхраняват, както следва: съгласно Вътрешните правила за дейността на учрежденския архив на НИП; съгласно утвърдената Номенклатура на делата със сроковете на съхраняване; съгласно Наредбата за реда за организирането, обработването, експертизата, съхраняването и използването на документите в учрежденските архиви на държавните и общински институции.

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

(7) Данните от регистъра се обработват от служители от дирекция ФБСД, отдел „Юрисконсулти" или на служители от други административни звена, на които им е възложена конкретна задача по конкретна молба, жалба, заявление за достъп до обществена информация.

(8) Данни от регистъра могат да бъдат предоставяни на държавни институции с оглед изпълнение на нормативно задължение.

(9) Най-малко веднъж на две години се извършват периодични проверки за състоянието и целостта на личните данни, съдържащи се в регистъра и относно необходимостта от по-нататъшното обработване.

Чл. 19. Длъжностните лица нямат право да разпространяват информация за личните данни, станали им известни при изпълнение на служебните им задължения.

ГЛАВА ЧЕТВЪРТА
ПРЕГЛЕД НА ЛИЧНИТЕ ДАННИ. ДЕЙСТВИЯ СЛЕД ИЗТИЧАНЕ СРОКА НА СЪХРАНЕНИЕ НА ДАННИТЕ В РЕГИСТЪРА

Чл. 20. (1) Проверките за състоянието и целостта на личните данни, съдържащи се във всеки регистър, се извършва от определени от главния секретар длъжностни лица от дирекциите, поддържащи съответния регистър. Определените лица изготвят доклад, който освен констатации за състоянието на съхраняваните данни, съдържа и предложения за предприемане на допълнителни организационни и технически мерки за защитата на личните данни, включително и предложение за прекратяване на обработването им.

(2) Проверката се извършва периодично, поне веднъж в годината или инцидентно при изменения на нормативните изисквания, при организационни и структурни промени в дейността на Института, които биха повлияли върху сигурността и поддържането на регистрите или при докладвани съмнения за сигурността на обработваните данни, или в други случаи по преценка на главния секретар.

(3) Резултатите от проверката се свеждат до знанието на длъжностното лице по защита на личните данни, които при необходимост правят предложения за предприемане на организационни и технически мерки чрез главния секретар до директора на НИП.

Чл. 21. (1) Необходимостта от по-нататъшното обработване на лични данни се преценява след извършване на проверка за състоянието и целостта на личните данни, съдържащи се в регистрите. Проверката се извършва не по-късно от един месец след утвърдения срок за съхранение на данните, съобразно утвърдената номенклатура на НИП или в инцидентно за при необходимост.

(2) Проверката се извършва от комисия, назначена със заповед на главния секретар на НИП. В състава на комисията се включват лица от административното звено, което обработва данните, един експерт-юрисконсулт от отдел „Юрисконсулти” и един служител с компетентност в информационните технологии.

(3) За работата на комисията по ал. 2 се съставя доклад. Докладът трябва да включва преценка на необходимостта за обработка на наличните данни или унищожаване. Докладът се предава на постоянно действаща експертна комисия, създадена в изпълнение на Наредбата за реда за организирането, обработването, експертизата, съхраняването и използването на документите в учрежденските архиви на държавните и общински институции. Същата изготвя акт за унищожаване, който се изпраща в Централен държавен архив, като след потвърждаването му съответните документи подлежат на унищожаване.

(4) 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 НИП възлага на изпълнител тези действия с договор с предмет конфиденциално унищожаване на документи.

ГЛАВА ПЕТА
ТЕХНИЧЕСКИ И ОРГАНИЗАЦИОННИ МЕРКИ ЗА ЗАЩИТА НА ДАННИТЕ

Чл. 22. Физическата защита на личните данни се осъществява при спазване на следните мерки:

1. сградата на НИП е зона с контролиран достъп на външни лица;
2. личните данни се обработват на работните места на лицата, които по функционални задължения или с изрично разпореждане обработват данни от определени регистри;
3. всички документи на хартиен носител, съдържащи лични данни, се съхраняват в заключени шкафове на работните места на упълномощените лица;
4. помещенията, в които се обработват лични данни, са оборудвани със заключване на вратите. Сградата на НИП е оборудвана с пожарогасителни средства и пожароизвестителна система. Сградите на НИП се охраняват денонощно от физическа охрана;
5. елементите на комуникационно-информационните системи, използвани за обработване на лични данни, се намират в помещение с ограничен достъп;
6. външни лица имат достъп до помещенията, в които се обработват лични данни, само в присъствието на отговорни за обработването служители.

Чл. 23. Персоналната защита на личните данни се осъществява при спазване на следните мерки:

1. лицата, обработващи лични данни, са длъжни да познават Общия регламент за защита на данните, Закона за защита на личните данни, настоящите, вътрешните правила и актове на НИП, уреждащи процесите по обработване на личните данни;
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 от преките си ръководители за рисковете за личните данни, обработвани от администратора.

Чл. 24. Документалната защита на личните данни се осъществява при спазване на следните мерки:

1. регистрите с лични данни, обработвани от НИП, се поддържат на хартиен или електронен носител;
2. обработването на личните данни се извършва в рамките на работното време на НИП;
3. достъп до регистрите с лични данни, обработвани от НИП, имат само служители, със задължение за обработване на данните, при спазване на принципа „Необходимост да се знае”;
4. личните данни се събират само за конкретни цели, в съответствие с нормативните изисквания към НИП;
5. сроковете за съхранение на личните данни от различните регистри е определен в утвърдената Номенклатура на делата със срокове за съхранение в НИП;
6. личните данни могат да бъдат предоставяни от отговорните служители само ако е необходимо за изпълнение на служебни задължения или ако са изискани по надлежния ред от държавни органи или упълномощени лица;
7. проекти на документи, които не са финализирани, 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).

Чл. 25. Защитата на автоматизирани информационни системи и мрежи се осъществява при спазване на следните мерки:

1. При работа с данните от регистрите, поддържани от НИП, се използват съответните софтуерни продукти за обработване. Данните се въвеждат в база данни и се съхраняват на сървър. Всеки упълномощен служител има личен профил (защитен с потребителско име и парола), с определени съобразно задълженията му права и нива на достъп. Дефинират се и уникални потребителски имена и пароли за стартиране на операционна система за 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. За защита на данните се инсталира антивирусна програма и се извършва периодична профилактика на софтуера и системните файлове.

3. За всички компютърни конфигурации, сървъри и комуникационни средства, от които зависи правилното поддържане на базите данни, се осигуряват непрекъсваеми токозахранващи устройства (UPS).

4. В помещенията, в които са разположени компютърни и комуникационни средства, се осигурява заключване на помещенията, система за ограничаване на достъпа, сигнално-охранителна система.

5. Организационни мерки за гарантиране нивото на сигурност:

а) осигуряване на охрана на сградата от физическа денонощна охрана;

б) забранено е използването на преносими лични носители на данни;

в) работните компютърни конфигурации, както и цялата IT инфраструктура, включително и достъпът до интернет, се използват единствено за служебни цели;

г) при ремонт на компютърна техника, на която се съхраняват лични данни, предоставянето ѝ на сервизната организация се извършва без устройствата, на които се съхраняват лични данни.

6. Отдалечен достъп до данни от регистрите се осъществява само от обработващи лични данни, в случаите когато НИП има сключени договори с тях.

Чл. 26. 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.

ГЛАВА ШЕСТА
ОБРАБОТВАЩ ЛИЧНИ ДАННИ

Чл. 27. (1) Националният институт на правосъдието като администратор на лични данни може да възложи обработване на лични данни от свое име само на обработващи лични данни, които следва от своя страна да предоставят достатъчни гаранции, че ще прилагат подходящи технически и организационни мерки по такъв начин, че обработването да отговаря на изискванията на закона.

(2) Националният институт на правосъдието организира възлагането на обработването на лични данни по начин, който да ограничи включването в обработването на други лица, освен определения обработващ. Обработването на лични данни се извършва само с изрично писмено възлагане от администратора, и то на конкретни субекти и техни данни.

(3) Обработването от страна на обработващия лични данни се урежда с договор с администратора. Възлагането на обработването се извършва само в случаите, когато е необходимо за осъществяване на предмета на договор. В договора за възлагане на обществена поръчка, когато е необходимо предоставяне на лични данни от изпълнителя по договор за възлагане на обществена поръчка, който е и обработващ на лични данни, се включва раздел за задълженията на обработващия лични данни, който съдържа задължения за обработващия личните данни, че:

1. действа единствено по указания на администратора;

2. гарантира, че лицата, оправомощени да обработват личните данни, са поели задължение за поверителност или са задължени по закон да спазват поверителност;

3. подпомага администратора с всички подходящи средства, за да се гарантира спазването на правата на субекта на данни;

4. по избор на администратора изтрива или връща на администратора всички лични данни след приключване на действието на договора за възлагане на обществена поръчка, освен ако правото на Европейския съюз или законодателството на Република България не изисква съхранение на личните данни;

5. предоставя на администратора цялата информация, необходима за доказване на спазването на изискванията на закона и договореното в договора;

6. спазва ограниченията за предоставяне на личните данни на друг обработващ

(4) В договора за възлагане се уговарят и санкции и отговорности при нарушения от страна на обработващия, свързани със защита на личните данни.

ГЛАВА СЕДМА
ОЦЕНКА НА ВЪЗДЕЙСТВИЕТО ВЪРХУ ЗАЩИТАТА НА ДАННИТЕ

Чл. 28. (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 НИП. Оценка на въздействието се извършва за високорискови дейности по обработване.

(2) Оценка на въздействието е необходимо при:

1. първоначалното въвеждане на нови технологии;

2. автоматизирано обработване, включително профилиране или автоматизирано вземане на решения, ако такива се въведат за работа в НИП;

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 Общия регламент.

(3) Оценката на риска съдържа най-малко:

1. системен опис на предвидените операции по обработване и целите на обработването за постигането на 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, предвидени за справяне с рисковете, включително гаранциите, мерките за сигурност и механизмите за осигуряване на защитата на личните данни.

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

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

ГЛАВА ОСМА
Процедура по докладване и управление на инциденти

Чл. 29. (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 Общия регламент, служителят, констатирал това нарушение/инцидент, незабавно докладва за това на прекия си ръководител и своевременно 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 по защитата на личните данни 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. Инцидентът се регистрира в регистъра по чл. 31 от настоящите правила от определеното със заповед на директора на НИП длъжностно лице.

(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. 30. (1) В случай че нарушението на сигурността създава вероятност от риск за правата и свободите на физическите лица, чиито данни са засегнати, 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. 31. (1) 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.

(2) Длъжностното лице по защита на личните данни уведомява главния секретар и директора на НИП за установените нарушения на сигурността на личните данни.

ЗАКЛЮЧИТЕЛНА РАЗПОРЕДБА

§ 1. Вътрешните правила се издават в изпълнение на чл. чл. 59, ал. 1 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 при обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО.

§ 2. Организацията и кнтрола по изпълнението на вътрешните правила се възлага на главния секретар.