Политики за поверителност на Сдружение „Национална мрежа за децата“

I. ПРАВНО ОСНОВАНИЕ

Чл.1 Настоящите правила се издава на основание чл. 23, ал. 4 от Закона за защита на личните данни (посл. изм. ДВ. бр.57 от 13 Юли 2007г.), Наредба за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни и Регламента (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) (ОВ L 119, 4.5.2016 г., стр. 1—88)

II. ЦЕЛИ НА ПРОЦЕДУРАТА

Чл.2 Настоящата процедура има за цел да регламентира:
1. механизмите на водене, поддържане, съхранение, заличаване и защита на регистри на лични данни, водени от Сдружение Национална мрежа за децата

2. задълженията на длъжностните лица, обработващи лични данни, и тяхната отговорност при неизпълнение на тези задължения;
3. необходимите технически и организационни мерки за защита личните данни на посочените по-горе лица от неправомерно обработване.

III. АДМИНИСТРАТОР И ОБРАБОТВАЩ НА ЛИЧНИ ДАННИ

Чл.3 (1) Администратор на лични данни е **Сдружение Национална мрежа за децата**, седалище и адрес на управление: бул. Витоша 52, ет. 4 представляван от Георги Василев Богданов.

(2) Оправомощено лице за работа с лични данни (обработващ данните) е всяко физическо или юридическо лице, на което администраторът е възложил да изпълнява задълженията, вменени му по силата на Закона за защита наличните данни.

(3) Отношенията между администратора и обработващия лични данни се уреждат с нормативен акт, писмен договор или с друг акт на администратора, в който се определя обемът на задълженията, възложени от администратора на обработващия данните.

(4) Администраторът може да определи повече от един обработващ личните данни като между отделните лица следва да съществува правна връзка.

(5) Ако счетоводството на дружеството се води от външно предприятие или физическо лице в облигационни отношения с администратора се счита, че с подписването на договор за счетоводно обслужване на същото е възложено да бъде обработващ

данните по регистрите, водени от администратора по силата на нормативен акт в качеството му на данъчно и осигурително задължено лице.

(6) Упълномощеното лице от ал. (5) може да води регистъра и да съхранява документите в офис на администратора или в собствено помещение като спазва настоящата процедура за защита на личните данни.

(7) Всички лица, от които се събират данни следва при поискване да бъдат уведомени, за името на обработващия и за адреса, на който се съхраняват личните данни ако той е различен от адреса на администратора.

(8) Всички лица, които имат достъп до и/или обработват лични данни на Сдружението, следва да преминат през инструктаж, да се запознаят подробно с процедурата и да се съгласят на пълна конфиденциалност спрямо нещата, станали им известни в следствие на достъпа до лични данни. За да удостоверят това те подписват декларация за съгласие Приложение N2 към настоящата процедура.

IV. РЕГИСТЪР НА ЛИЧНИ ДАННИ

Чл. 4 Видовете регистри, водени от **Сдружение Национална мрежа за децата** са изброени в приложение 1, което е неразделна част от тази процедура. В описанието на всеки регистър в Приложение 1 е включено конкретното нивото на чувствителност на обработваните данни и други препратки към приложимите членове от вътрешните правила.

V. НИВА НА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

Чл. 5 Нивата на защита на личните данни са начално, средно, високо.

VI. МЕРКИ ПРИ НАЧАЛНО НИВО НА ЗАЩИТА

Чл. 6 Мерките за защита, класифицирани при ниско ниво на защита се предприемат за всички регистри с лични данни, обработвани само на хартиен носител.

Чл. 7 (1) Регистрите с ниско ниво на защита са подредени в картотечни папки в шкаф в работно помещение със заключване.

(2) Копие от ключа за работното помещение, където се съхраняват регистрите имат само оправомощените за достъп до регистъра лица.

Чл. 8 (1) Оправомощени да работят с регистъра са само онези лица, на длъжности, описани в настоящата процедура или приложенията към нея или за който има издадена заповед от ръководството на **Сдружение Национална мрежа за децата**

(2) Ръководството не може да оправомощава лица, чиито задължения не изискват задължително работа със съответния регистър.

(3) Лицата, оправомощени да боравят с регистъра, отговарят за спазването на ограниченията за достъп до него на неоправомощени лица и са персонално отговорни пред управителя за нарушаването на разпоредбите, освен в случаите на форсмажорни обстоятелства.

VII. МЕРКИ ПРИ СРЕДНО НИВО НА ЗАЩИТА

Чл. 9 Мерките за защита, класифицирани при начално и средно ниво се предприемат за всички регистри с лични данни, обработвани на хартиен и технически носител, в компютърна система на локален компютър или в мрежа, несвързани с обществената мрежа.

Чл. 10 За регистрите със средно ниво на защита са валидни всички мерки, задължителни при ниско ниво.

Чл. 11 (1) Данните се обработват на компютър, чиято операционна система се стартира с парола.

(2) Всяко оправомощено за работа с регистъра лице има собствен акаунт на компютъра, на който се води регистъра и отделна парола за него.

(3) По преценка на обработващия данните, ако регистъра се води не чрез специална програма, която се стартира чрез парола, а във вид на електронни таблици или текстови документи всяка таблица/документ да бъде защитена срещу четене и промяна чрез парола, известна само на оправомощените лица.

Чл. 12 (1) Администраторът на личните данни в лицето на изпълнителния директор на **Сдружение Национална мрежа за децата** извършва периодични проверки за спазването на правилата за достъп и съхраняване на регистрите и при наличието на установено нарушение наказва дисциплинарно виновните лица.

(2) Администраторът съставя протокол за направената проверка и констатираните нарушения, който при поискване може да бъде представен в Комисията по защита на личните данни.

(3) Проверките по ал. 1 се провеждат минимум веднъж годишно.

VIII. МЕРКИ ПРИ ВИСОКО НИВО НА ЗАЩИТА

Чл.13 Мерките за защита, класифицирани при начално, средно и високо ниво се предприемат за всички регистри с лични данни, обработвани на хартиен и технически носител, в компютърна система на локален компютър или в мрежа, свързани с обществената мрежа.

Чл. 14 За регистри с високо ниво на защита се спазват всички правила, приложими за регистри с ниско и средно ниво както и допълнителните правила, описани в тази точка.

Чл. 15 (1) Задължителната информация, която следва да бъде регистрирана при високо ниво на защита е: идентичност на служителя, дата на достъп, регистъра, за който е получен достъп, вида на достъпа и кога достъпа е бил отказан.
(2) Извън информацията по ал.1 администраторът регистрира и информация, която позволява да се идентифицира записа, до който е имал достъп служителят.
(3) Информацията по ал. 1 и 2 се съхранява за период най-малко от две години.
(4) Администраторът отговаря за извършване на редовни проверки на записаната информация по контрола и изготвя отчет за тях минимум веднъж на всяко тримесечие.

Чл. 16 При обработване на лични данни по смисъла на чл. 5 във връзка с ал. 1 от закона се предприемат допълнителни мерки, свързани с разпространението им по

телекомуникационни мрежи, под формата на криптиране или използване на друг механизъм, гарантиращ, че данните са нечетливи или не са променени.

IX. ПРОЦЕДУРИ ЗА СЪЗДАВАНЕ НА АРХИВНИ КОПИЯ И ПЛАНИРАНО И ПОИСКАНО УНИЩОЖАВАНЕ НА ДАННИ ОТ РЕГИСТРИТЕ

Чл. 17 (1) Създаването на архивни копия от регистрите е допустимо само ако не са отпаднали целите, за които е бил създаден регистъра или законоустановения срок на поддържането на данните.

(2) Архивни копия се създават само с цел предпазване на данните от загубване и/или не планирано унищожаване.

(3) Архивните копия трябва да съдържат количеството информация, необходимо за реконструирането им в състоянието, в което са били по време на изгубването или унищожаването им.

(4) Регистрите се архивират на хартиен, технически или електронен носител с периодичност, определена от администратора, съобразно интензивността на въвеждане на нови данни.

(5) Архивните данни се съхраняват в същото или в друго работно помещение в шкаф с ограничен достъп, до който имат достъп само лица, оправомощени да работят със съответния регистър.

(6) Лицата, които отговарят за съхранението на оригинала на регистъра и недопускането на достъп до него на неоправомощени лица, отговарят и за съхранението на всички архиви.

Чл.18 (1) Регистрите или части от тях се унищожават по подходящ начин веднага след отпадане на целите, за които са били създадени или след изтичане на законоустановения срок за съхранението на архивни копия.

(2) Унищожаването се извършва само от администратора или от изрично оправомощените да работят със съответния регистър лица. Последните съставят **протокол** за унищожението на регистъра, в който дават кратко описание на унищожените данни (без да оповестява лични данни от него), начина на унищожението им и удостоверяват чрез подписа си, че след предприетите действия данните от регистъра са заличени и/или унищожени.

(3) Всички архивни копия се унищожават заедно с оригиналните документи от регистъра според процедурата по ал. 1 и ал. 2 или се предават на съответните институции или администратори на лични данни, ако това е предвидено в нормативен акт.

(4) Временни файлове се съхраняват при същите условия както регистрите, за които се отнасят и се унищожават веднага след изпълнението на предназначението им.

Чл. 19 След унищожаването на регистъра и копията от него се допуска запазване единствено на обобщена информация за статистически, исторически или научни цели в съответствие с разпоредбите на Закона за защита на личните данни.

Чл. 20 Ако лице, чиито данни са част от регистри, водени от Сдружение желае неговите данни да бъдат унищожени, той/тя подава официално заявление (в писмена форма) на хартия или на мейл адреса (office@nmd.bg). След получаване на заявлението, данните на лицето следва да бъдат заличени, съобразно ал.1 и ал 2. Ако закона предвижда друго (в случаите, когато се отнася за наети служители и/или контрагенти по договори), администратора на лични данни следва да уведоми лицето пожелало данните му да бъдат заличени, кои от тях няма да бъдат, цитирайки законовото основание за това.

X. МЕРОПРИЯТИЯ ЗА ЗАЩИТА НА ТЕХНИЧЕСКИТЕ И ИНФОРМАЦИОННИТЕ РЕСУРСИ ПРИ АВАРИИ, ПРОИЗШЕСТВИЯ И БЕДСТВИЯ

Чл. 21 (1) Сдружението се стреми да избягва поддържането на регистри само на хартиен носител. Когато това е невъзможно при наличието на подходящо помещение до което имат достъп само оправомощени лица и шкаф с ограничен достъп да се води архивно копие на хартиените носители на регистъра.

(2) При периодичния инструктаж за правилата за безопасност в офис помещенията и действията на служителите при авария, произшествие или бедствие се инструктират и оправомощените лица как да изнесат архивните копия на регистрите без риск за живота им.

(3) При предупреждения за настъпващи природни бедствия и евакуирането на живущите и работещите в застрашените райони, оправомощените за достъп лица полагат максимални усилия, без да застрашават живота си, за да отнесат със себе си архивни копия на регистрите.

(4) Като последна мярка е възможно данните да бъдат криптирани и защитени от парола, известна само на оправомощеното лице и прехвърлени по електронен път на сървър или друг администратор на лични данни, намиращ се извън застрашената от бедствие област като се спазват изискванията на Закона за защита на личните данни за предаване на криптирана информация. Веднага след възобновяване на нормален работен режим криптираното копие следва да бъде унищожено, а регистъра-възстановен в предишния му вид.

XI. РЕД НА ЗАДАВАНЕ, ИЗПОЛЗВАНЕ И ПРОМЯНА НА ПАРОЛИ, КАКТО И ДЕЙСТВИЯ В СЛУЧАЙ НА УЗНАВАНЕ НА ПАРОЛА И/ИЛИ КРИПТОГРАФСКИ КЛЮЧ

Чл. 22 (1) Пароли имат задължително операционната система на компютрите, на които се водят или съхраняват регистрите, като всеки оправомощен има собствен акаунт и парола за него независимо, дали на един компютър и с един файл може да работят повече от едно лице.

Чл. 23 (1) Пълен списък с паролите на всички оправомощени има единствено администратора на лични данни в лицето на неговия законен представител.

(2) Пълният списък се съхранява или на хартиен носител, или на електронен носител при най-високите приложими мерки за сигурност.

Чл. 24 Паролите за достъп се променят периодично, но не по-късно на всеки 6 месеца.

Чл. 25 (1) Инциденти с достъп до данните на неоторизирани лица, включително узнаване на парола и разбиване на криптографски ключ се докладват писмено до управителя на Сдружението от лицето, което ги е установило до един ден от датата на установяването им.

(2) Писмената докладна за настъпил инцидент по ал. 1 съдържа минимум кратко описание на вида на данните, който са били разкрити, времето на настъпването на инцидента, ако е известно, времето на установяването му, трите имена, длъжност и подпис на лицето, което го докладва, трите имена и длъжност на лицето, на което е бил докладван, последствията от него и мерките за отстраняването му (предприети или предложени).

(3) Администраторът предприема действия по подобряване на сигурността на данните, предотвратяване на повторното разкриване на информацията и наказва дисциплинарно виновните лица ако има такива.

(4) Лицето, което е констатирало узнаването на паролата и/или криптографския ключ незабавно я/го променя с цел да предотврати изтичането на лични данни или уведомява оправомощените за това лица устно или писмено.

(5) Ако узнаването на паролата и/или криптографския ключ представлява престъпление се уведомяват незабавно и компетентните държавни органи.

Чл. 26 (1) Администратора или упълномощени от него лица редовно провеждат профилактика на компютърните и комуникационните средства, включваща и проверка за вируси, за нелегално инсталиран софтуер, на целостта на базата данни, с цел предотвратяване от злонамерено узнаване на паролите от външни лица.

(2) На компютрите, на които се съхраняват лични данни от регистрите е инсталирана актуална версия на антивирусна програма и да се прави профилактично сканиране минимум един път месечно.

XII. ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

Чл. 27 (1) Настоящите правила влизат в сила от 15.05.2019г.