ИНСТРУКЦИЯ
ЗА ПРАКТИЧЕСКОТО ОСЪЩЕСТВЯВАНЕ НА НАДЗОРНАТА ДЕЙНОСТ НА КОМИСИЯТА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

СЪДЪРЖАНИЕ:

I. СЕКТОРНИ ПРОВЕРКИ / ПЛАНОВИ ПРОВЕРКИ / ОДИТИ – ДИРЕКЦИЯ „ППН“, ОТДЕЛ „КАНП“

1. Неприсъствени действия / Планиране / Предварителна подготовка

1.1. Критерии за избор на секторна проверка:

1.1.1. обществена значимост на нарушенията,сигнализирани с жалби и сигнали;

1.1.1. повтаряемост на нарушенията в определен сектор;

1.1.1. промяна на законодателството в определен сектор;

1.1.1. въвеждане на нови технологии и услуги,предоставяни от АЛД/ОЛД, включващи обработване на личните данни;

1.1.1. други…….

1.2. Предварителен анализ на сектора:

1.2.1. анализ от служителите на отдел „КАНП“ по горепосочените критерии, както и предварително проучване на субектите на сектора, в т.ч. има ли подадени жалби, сигнали, уведомления в КЗЛД и откази от съдействие, издадените АУАН и НП;

1.2.2. анализът завършва с изготвяне на докладна записка, която включва предложение за извършване на проверка в конкретния сектор, както и предмета, обхвата и целите на проверката;

1.2.3. докладната записка се внася за разглеждане и приемане на заседание на КЗЛД с предложение за членовете на екипите за проверки и привличане на външен експерт (при необходимост);

1.2.4. приемане на Решение на КЗЛД за извършване на проверка с определяне на предмета, обхвата, субектите и целите на проверката, вкл. привличане на външен експерт (при необходимост).

1.3. Планиране на Секторната проверка / Плановата проверка / Одита:

1.3.1. издаване на заповеди за проверка – два оригинала;

1.3.2. разписване на функции и отговорности на членовете на екипите за проверки;

1.3.3. изготвяне на хронограма за действията на екипа (при необходимост);

1.3.4. проучване на приложимото към сектора законодателство и насоките на Европейския комитет по защита на данните;

1.3.5. проучване на приложима към сектора практика – на КЗЛД, на Съда на Европейския съюз;

1.3.6. справки публични бази данни;

1.3.7. справки интернет страници;

1.3.8. телефонни разговори;

1.3.9. електронни съобщения;

1.3.10. изискване на становище/становища;

1.2.11. изпращане на уведомителни писма до АЛД/ОЛД за проверката с приложени въпросници, включително и по електронен път.

2. Проверка на място

2.1. легитимиране на проверяващия екип със служебни карти;

2.2. легитимация на представляващия АЛД/ОЛД;

2.3 връчване на заповедта на председателя на КЗЛД за извършване на проверката – връчва се оригинал на заповедта, като на екземпляра на проверяващия екип АЛД/ОЛД или упълномощеното от него лице собственоръчно написва текст, че е получил копие от заповедта за проверка, датата, трите си имена и подпис (за юридическите лица – печат, при възможност);

2.4. задължителна проверка и събиране на доказателства относно:

2.4.1. спазване принципите за законосъобразно обработване на лични данни (чл. 5 и 6 от Регламент (ЕС) 2016/679);

2.4.2. условията за даване на съгласие (чл. 7 от Регламент (ЕС) 2016/679);

2.4.3. условията, приложими за съгласието на дете във връзка с услугите на информационното общество (чл. 8 от Регламент (ЕС) 2016/679);

2.4.4. обработването на специални категории лични данни (чл. 9 от Регламент (ЕС) 2016/679);

2.4.5. предприетите от АЛД/ОЛД действия за информиране на физическите лица за целите на обработване на личните им данни и упражняването на техните права, съгласно чл. 15–22 от Регламент (ЕС) 2016/679;

2.4.6. предаване на лични данни на трети държави или международни организации (чл. 44–50 от Регламент (ЕС) 2016/679) – на кои, основанието и начин на предаване, категории лични данни, технически и организационни мерки за защита;

2.4.7. обмен на лични данни с български институции – на кои, основанието и начин на предаване, категории лични данни, технически и организационни мерки за защита;

2.4.8. предприетите технически и организационни мерки за защита на личните данни;

2.4.9. наличие на одити по отношение спазването на Наредбата за минимални изисквания за мрежова и информационна сигурност и ISO 27701;

2.4.10. проверка на сигурността и сертифициране на информационните системи, обработващи лични данни;

2.4.11. наличие на сертификати за информационна сигурност и за защита на личните данни;

2.4.12. присъединил ли се е АЛД/ОЛД към одобрен кодекс за поведение.

2.5. събиране на доказателства за всеки установен факт – документи на хартиен и/или електронен носител (в т.ч. направения анализ на риска и определяне на нивото на въздействие, правила, процедури, становища, екранни разпечатки и др.), като задължително АЛД/ОЛД предоставя заверени копия на сключени договори с физически или юридически лица, касаещи обработването на лични данни;

2.6. изготвяне на констативен протокол по време на проверката, екземпляр се връчва на АЛД/ОЛД;

2.7. изготвяне на приемо-предавателен протокол със заверени копия на документи и предоставени доказателства от АЛД/ОЛД, екземпляр се връчва на АЛД/ОЛД;

2.8. указване на срок за предоставяне на допълнителни документи (при необходимост).

3. Приключване на проверката на място

3.1. анализ на събраните в хода на проверката документи, в т.ч. Насоките на Европейския комитет по защита на даннитеи решенията на Съда на Европейския съюз, приложими към сектора;

3.2. анализ на сключените договори с физически или юридически лица и наличието на клаузи, регламентиращи обработването на личните данни;

3.3. изготвяне на констативен акт и завеждането му в деловодната система, ведно с приложените в оригинал документи и доказателства, като задължително включва мнение и предложения на проверяващия екип:

3.3.1 предложение за приемане при липса на нарушение;

3.3.2. предложение за издаване на корективна мярка по чл. 58, § 2 от Регламент (ЕС) 2016/679;

3.3.3. при установяване на административно нарушение – предложение за налагане на санкция на отделните субекти, обект на Секторната проверка / Плановата проверка / Одита, стартиране на производство по ЗАНН със съставяне и връчване на АУАН.

3.4. приемане с решение на изготвените констативни актове.

4. Приключване на Секторната проверка / Плановата проверка / Одита

4.1. изготвяне на окончателен доклад за Секторната проверка / Плановата проверка / Одита, съдържащ анализ на сектора, заключения и предложение до КЗЛД за изготвяне на препоръки към всички субекти в сектора (при необходимост);

4.2. внасяне на окончателния доклад за разглеждане и приемане на заседание на КЗЛД.

5. Последващи действия на КЗЛД

5.1. запознаване и приемане на окончателния доклад за Секторната проверка / Плановата проверка / Одита и одобрение на препоръки към всички субекти в сектора;

5.2. публикуване на анонимизиран окончателен доклад и препоръките на интернет страницата на КЗЛД;

5.3 изготвяне на писмо до съответните субекти в сектора с констатации от проверката (когато няма наложена корективна мярка);

5.4 при издаване на корективна мярка по чл. 58, § 2, б. „г“ от Регламент (ЕС) 2016/679:

5.4.1. Решение на КЗЛД – диспозитивът на Решението задължително съдържа издадената корективна мярка (разпореждане), срок за нейното изпълнение, срок за представяне на доказателства за изпълнението му от АЛД/ОЛД, информация за административно-наказателната отговорност, която носи АЛД/ОЛД в случай, че не го изпълни или не изпрати доказателства за изпълнението му в указания срок, както и за възможността за обжалване пред съответния съд;

5.4.2. Решението се връчва на съответните АЛД/ОЛД;

5.4.3. след изтичане на 14-дневен срок влиза в сила и подлежи на изпълнение, ако ответната страна не оспорва Решението;

5.4.4. предоставяне на писмени доказателства от АЛД/ОЛД за изпълнение на корективната мярка и докладване на заседание на КЗЛД;

5.4.5. ако в указания срок АЛД/ОЛД не представи доказателства за изпълнение на корективната мярка:

а) изпраща се напомнително писмо с обратна разписка с указан 7-дневен срок, в който АЛД/ОЛД следва да предостави доказателства и/или становище за изпълнение на решението на КЗЛД и нейните разпореждания, както и информация за административно-наказателната отговорност, която носи АЛД/ОЛД в случай, че не го изпълни;

б) при изпълнение на указаното с писмото, се изготвя докладна записка до КЗЛД с предложение за приемане;

в) в случай на неизпълнение на указаното с писмото, се изготвя докладна записка до КЗЛД с предложение за налагане на административна санкция по реда на чл. 83, § 6 от Регламент (ЕС) 2016/679 и чл. 84 от ЗЗЛД, която се докладва на КЗЛД.

г) вземане на Решение на КЗЛД.

5.4.6 издадените констативни актове се присъединяват към преписката;

5.4.7 издадените АУАН, НП и решенията за корективни мерки по чл. 58, § 2 от Регламент (ЕС) 2016/679 се вписват и съхраняват в съответния регистър.

II. СЪВМЕСТНИ ПРОВЕРКИ С ДРУГИ НАДЗОРНИ ОРГАНИ

А. Общи положения. Съвместни операции извън Република България.

1. Въведение

1.1. Настоящият документ акцентира главно върху член 62 от Регламент (ЕС) 2016/679. За да се интегрират разпоредбите на член 62 с общите разпоредби на регламента, се прави позоваване и на следните разпоредби на Регламент (ЕС) 2016/679:

1.1.1. Съображения: 125, 127, 134, 138

1.1.2. Членове: 55, 56, 57, § 1, б. ж), 60, 63, 66

1.2. Настоящото процедурно ръководство е придружено от две приложения:

1.2.1. Приложение I: Съдържа общ проект на съвместен оперативен план за действие.

1.2.2. Приложение II: Съдържа диаграми на случаите, илюстриращи обмена между участващите надзорни органи в съвместна операция в два сценария: със и без водещия надзорен орган.

2. Определение: съвместна операция възниква, когато два или повече надзорни органа обединяват усилията си, за да действат по общо договорена цел. За целта, надзорните органи предоставят на разположение своите ресурси, включително техните умения и персонал.

3. Участници

3.1. Сътрудничеството между надзорните органи може да приема различни форми. В съответствие с Регламент (ЕС) 2016/679 надзорните органи са свободни да

участват в една или няколко форми на сътрудничество, в зависимост от техните нужди и целта, която възнамеряват да постигнат.

3.2. Съвместна операция може да бъде проведена или от надзорните органи, които си сътрудничат по национален казус (на доброволни начала), както и от засегнатия надзорен орган, която ръководи случай на местно ниво съгласно чл. 56, § 5, или от надзорния орган, които работят заедно по механизма за обслужване на едно гише под егидата на водещия надзорен орган:

3.2.1 Съвместна операция между надзорните орган, които си сътрудничат по национален случай съгласно чл. 55 (на доброволни начала): надзорният орган, инициращ съвместна операция, има свободата да избере да включи всеки друг надзорния орган в съвместната операция.

3.2.2. Съвместна операция между надзорния орган по механизма за обслужване на едно гише, който разглежда казуса на местно ниво съгласно чл. 56, § 2 и чл. 56, § 5.

3.2.3. Съвместна операция между надзорните органи по механизма за обслужване на едно гише в съответствие с чл. 56, § 1 (по инициатива на водещия надзорен орган): когато съвместната операция е насочена към трансгранична обработка на лични данни, водещият надзорен орган трябва да търси участието на всички надзорни органи с право на участие.

3.3. Надзорните органи с право на участие са:

3.3.1. Надзорният орган на държава членка, където значителен брой субекти на данни е вероятно да бъде съществено засегнат от операциите по обработка.

3.3.2. Надзорният орган на държавата членка, където администраторът или субектът, обработващ данни, има ведомства.

3.3.3. Водещият надзорен орган може да се свърже с други надзорни органи, които счита за подходящи, включително органи, които са получили жалби, свързани със съвместната операция.

3.4. Във всеки случай всеки друг надзорен орган може да бъде поканен да участва в съвместната операция, ако може да допринесе с определен ресурс за успеха на съвместната операция.

3.5. Участващите надзорни органи трябва да си сътрудничат активно за определяне на план за действие, както е описано в приложение „План за действие за съвместна операция“, който е реалистичен и ефективен, като се вземат предвид ограничения като ресурси, време, разходи и др. По този начин, например, в случаите, в които голям брой надзорни органи желаят да участват в съвместната операция надзорните

органи трябва да се стремят да се споразумеят за определянето на намален екип от персонала, който да изпълнява всяко конкретно действие, предвидено в съвместната операция.

3.6. Тъй като чл. 62 не предвижда срокове, нито какъвто и да е конкретен метод за организиране на съвместни операции, настоящото процедурно ръководство съдържа някои разпоредби за разглеждане на тези аспекти в точка 5 – „Общи условия между участващите надзорни органи и приложения „План за действие за съвместна операция“ и II.

4. Процедура

4.1. Идентифициране на участниците в съвместна операция - без срок

4.1.1. Иницииращият надзорен орган съобщава за възможната операция, като споделя цялата необходима информация. Съвместните операции се инициират официално на ИТ платформите на ЕКЗД.

4.1.2. В отговор заинтересованите надзорни органи отговарят на инициативата на надзорния орган.

4.2. Изпращане на покана за участие в съвместна операция: съответните елементи от плана за действие в приложение 1 могат да се използват като образец за покана за участие в съвместната операция. Тази покана може да бъде изпратена чрез ИТ платформите на ЕКЗД

4.2.1. При трансгранична обработка – срок без закъснение в рамките на един месец

а) водещият надзорен орган отправя покана до останалите надзорни органи за участие в съвместната операция, включително най-малко тези надзорни органи, които имат право да участват в съответствие с чл. 62, § 3. Той също така отговаря на исканията на надзорни органи, които желаят да участват.

б) водещият надзорен орган продължава да предава основна информация по случая на надзорните органи, определени като „незасегнати", за да установи колкото се може повече надзорни органи с право на участие, за да ги включи в процеса на подготовка на съвместната операция.

в) в случай, че водещият надзорен орган не спази задължението да покани в рамките на един месец или да отговори незабавно на заявките за участие, другият надзорен орган може да приеме временна мярка на територията на своите държави членки – задействане на процедурата по спешност и изискването на спешно становище

или спешно решение със задължителен характер от ЕКЗД (чл. 62, § 7 и чл. 66 от Регламент (ЕС) 2016/679).

4.2.2. В други случаи (вж. чл. 55 или чл. 56, § 5), инициаторът на съвместната операция кани всеки надзорния орган, който желае да включи в операцията – срок в рамките на един месец

а) инициращият надзорния орган изпраща покани на всички надзорни органи, които желае да включи и отговаря на исканията на надзорния (те) орган (и), който/които желае/желаят да участва (т).

4.3. Споразумение за „План за действие за съвместна операция“ между участващите надзорни органи - без срок

4.3.1. Надзорните органи, участващи в съвместна операция, се договарят относно целта (ите), естеството (ата), ресурсите, продължителността, условията и т.н. на плана за действие на съвместната операция, преди той да стартира официално.

4.3.2. Конспект за възможен план за действие за съвместна операция се предлага в приложение План за действие за съвместна операция

4.4. Същност на правомощията, упражнявани от командированите членове и служители на надзорния (те) орган (и) - без срок

4.4.1 За всяка съвместна операция, включваща пряко участие на членове и персонал на надзорния орган на територията на друга държава, приемащият надзорен орган може да предостави същите правомощия на командированите членове или персонал на командироващия надзорен орган, участващи в съвместна операция, както на собствените си членове и персонал.

4.4.2. Има две условия, които трябва да бъдат изпълнени:

а) националното законодателство на приемащия надзорен орган позволява това.

б) командироващият надзорен орган разрешава предоставянето на правомощия на своите членове и персонал.

4.4.3. Като алтернатива и само за разследващи действия, приемащият надзорен орган може да приеме, че членовете и служителите на командироващия надзорен орган упражняват свои собствени правомощия за разследване.

4.4.4. Има две условия, които трябва да бъдат изпълнени:

а) националното законодателство на приемащия надзорен орган позволява това.

б) упражняването на такива разследващи правомощия се извършва под ръководството и в присъствието на приемащия надзорен орган (персонал или членове).

4.4.5. Като цяло, и особено преди съвместна операция, надзорните органи трябва да определят в рамките на съответните си организации всички съответни процедури за предоставяне на правомощия на членове и персонал на командироващия надзорен орган.

4.4.6. Съвместни операции, включващи пряко участие на членове и персонал на надзорния орган на територията на друга държава, ще се извършват под ръководството и инструкциите на приемащия надзорен орган. (Процесуалното) право, приложимо за съвместни операции, е правото на държавата членка на приемащия надзорен орган.

4.5. Завършване на съвместна операция - без срок

4.5.1. При завършване на съвместна операция надзорните органи могат да обмислят споделянето на резултатите по начина, който считат за най-подходящ, като вземат предвид по-специално правните ограничения, приложими в приемащата държава членка на надзорния орган, дали да споделят информация с други надзорни органи или с обществеността.

5. Отговорност и наказателна отговорност в съвместна операция

5.1. Държавата членка на приемащия надзорен орган поема отговорност, включително наказателна отговорност, за всякакви вреди, нанесени от персонала на командироващия надзорния орган на нейна територия (чл. 62, § 4 от Регламент (ЕС) 2016/679).

5.2. По-специално, държавата членка на приемащия надзорен орган поправя всякакви вреди, причинени от персонала на командироващия надзорен орган, при същите условия, приложими за вреди, причинени от нейния собствен персонал.

5.3. Държавата членка на приемащия надзорен орган обикновено се въздържа от искане за възстановяване на суми от която и да е друга държава членка. Държавата членка на командироващия надзорен орган обаче е задължена да възстанови изцяло на държавата членка на приемащия надзорен орган всички суми, изплатени на имащите право да ги получат в резултат на вреди, причинени от персонала на командироващия надзорен орган на територията на държавата членка на приемащия надзорен орган (чл. 62, § 5 от Регламент (ЕС) 2016/679).

6. Общи условия и условия между участващи надзорни органи

Регламент (ЕС) 2016/679 съдържа много разпоредби, които подробно описват функциите, компетенциите и правомощията на надзорните органи, както и сътрудничеството между тях.

Чл. 62, заедно с членове 55, 56, 57, § 1, б. ж) и чл. 60, както и съображения 123, 127, 134 и 138 и настоящото ръководство, изготвено от ЕКЗД, описват контекста на съвместните операции с достатъчно ниво на детайлност, което прави ненужно определянето на конкретно официално споразумение или Меморандум за разбирателство за всяка съвместна операция. Може да е достатъчно надзорните органи, участващи в съвместната операция, да определят план за действие за съвместна операция, използвайки образеца в приложение План за действие за съвместна операция.

Накратко, Регламент (ЕС) 2016/679 е достатъчна правна основа за надзорните органи сами да позволят и прилагат механизми за сътрудничество и по-специално съвместни операции.

Следователно необходимостта от допълнителни уточнения е ограничена, за да включва само онези аспекти, които Регламент (ЕС) 2016/679 оставя на свободната воля на страните или са строго необходими в съответствие с действащите национални закони.

6.1. Общи оперативни аспекти

6.1.1. Регламент (ЕС) 2016/679 разглежда съвместните операции като механизъм за сътрудничество, включващ съвместни разследвания и съвместни мерки за прилагане, в които участват членове или служители на надзорните органи на други държави членки. Тази отворена концепция позволява да се обхванат различни видове действия в много широк смисъл. Всъщност настоящото ръководство определя съвместна операция, при която два или повече надзорни органа обединяват усилия, за да действат по общо договорена цел. За да го направят, надзорните органи предоставят техните ресурси, включително техните умения и персонал.

6.1.2. Участващите надзорни органи, в съответствие с разпоредбите на чл. 60, § 1 и чл. 57, § 1, б. „ж“), трябва да положат всички необходими усилия, да си сътрудничат и да обменят цялата съответна информация помежду си, за да завършат успешно съвместната операция.

6.1.3. В допълнение и в съответствие със съображение 125, в съвместни операции, в които има водещ или приемащ надзорен орган, ще бъде от съществено значение, в качеството си на ръководен или приемащ орган, този надзорен орган да включва и да координира останалата част от участващите надзорни органи в процеса на вземане на решения, които трябва да бъдат извършени, за да завърши успешно съвместната операция. Вземането на решения трябва да се разбира като всяко действие или резултат, който може да повлияе на по-късните етапи от цялостната процедура, включително съвместната операция.

6.1.4. Всеки надзорен орган, участващ в съвместната операция, изготвя и актуализира списък на своя персонал, участващ в тази операция.

6.1.5. Одитите или проверките на място се извършват в съответствие с националното законодателство на държавата, в която се извършва одитът или проверката. Приемащият надзорен орган ще отговаря за координирането и изготвянето на план за проверка, като се вземат предвид предложенията на участващите надзорни органи за постигане на консенсус. Приемащият надзорен орган трябва да вземе предвид различните условия, свързани с валидността на доказателствата, в съответствие със съответното национално законодателство на участващите надзорни органи, ако те са съвместими със закона на приемащия надзорен орган.

6.1.6. Когато личните данни се обработват в рамките на съвместната операция, участващите надзорни органи ще бъдат съвместни администратори за целите на такава обработка, тъй като те съвместно определят целите и средствата на обработката. Всеки участващ надзорен орган ще отговаря за спазването на задълженията, наложени от Регламент (ЕС) 2016/679 във връзка с обработваните лични данни и задълженията, определени в глава III от Регламент (ЕС) 2016/679.

6.1.7. Със съгласието на всички заинтересовани участници, всеки аспект, който не е предварително договорен, може да бъде договорен по всяко време по време на съвместната операция, както и всеки предварително договорен аспект може да бъде променян.

6.2. Продължителност на съвместната операция

6.2.1. Участващите надзорни органи ще решат с консенсус датите или етапите за началото и края на съвместната операция, както и всички последващи актуализации или модификации.

6.3. Поверителност, прозрачност и публичност

6.3.1. Без да се засягат разпоредбите, установени в съответните национални закони, участващите надзорни органи могат да се споразумеят с консенсус да оповестят публично съществуването на съвместната операция и информацията, свързана с нея.

6.3.2. В съответствие с чл. 54, § 2 от Регламент (ЕС) 2016/679, това задължение за поверителност се разпростира върху всички служители на надзорния орган, участващи в съвместната операция, и върху всички надзорния орган, които, макар и да не участват пряко в съвместната операция, имат достъп до информация, получена от съвместната операция като засегнати органи.

6.3.3. Участващите надзорни органи ще прилагат подходящи технически и организационни мерки, за да гарантират сигурност при обработката и обмена на

информация както по време на развитието на съвместната операция, така и след нейното приключване.

6.3.4. Освен това участващите надзорни органи ще прилагат подходящи механизми, за да гарантират поверителността на информацията, която е обект на търговска тайна или интелектуална собственост както по време на, така и след приключване на съвместната операция.

6.3.5. Участващите надзорни органи трябва да ограничат, доколкото е възможно, достъпа до информация, получена в резултат на съвместната операция, до персонала, участващ в съвместната операция (принцип *„необходимост да се знае“).*

6.3.6. Участващите надзорни органи уведомяват незабавно за всяко нарушение на посочените по-горе мерки за поверителност и сигурност другите участващи надзорни органи.

6.3.7. Участващите надзорни органи трябва да приемат, че информацията, споделена в рамките на съвместната операция, може да се наложи да бъде разкрита в съответствие с националното законодателство. Когато участващ надзорен орган получи искане за достъп до тази информация, той информира незабавно останалите участващи надзорни органи и ще вземе предвид, доколкото е възможно, становището на другите участващи надзорни органи в решението, взето в съответствие с действащите национални закони.

6.4. Съхранение и повторно използване на информацията

6.4.1. Информацията от съвместна операция ще се използва за конкретните разследвания, довели до съвместната операция, при условие че информацията е от значение за тези разследвания. Участващите надзорни органи ще съхраняват информацията, която включват в своите досиета, в съответствие с действащите национални закони.

6.4.2. В съответствие с действащите национални закони участващите органи могат да използват повторно информация, различна отлични данни, събрана по време на съвместната операция, за други различни разследвания, които могат да бъдат извършени при упражняване на техните правомощия. Повторното използване на лична информация следва да бъде ограничено до онези случаи, в които законодателството на Съюза или на държава членка може да определи и уточни задачите и целите, за които по-нататъшната обработка следва да се счита за съвместима и законна.

6.5. Език и преводи

6.5.1. При всяко действие (проверка на място, искане за информация и др.), извършено в рамките на съвместната операция, използваните езици ще бъдат

приспособени към нуждите на участниците: администратори, субекти, обработващи данни, трети страни, субекти на данни и др.

6.5.2. Участващите надзорни органи трябва да се споразумеят за работните езици в рамките на съвместната операция. Всеки надзорен орган, отговорен за всяко действие, ще осигури необходимите неофициални писмени преводи, за да сподели резултатите с останалите участващи надзорни органи.

6.5.3. Други писмени преводи (например: официални преводи на документи) или симултанни преводи (например: по време на проверка на място) трябва да бъдат платени и уредени от поръчващия (ите) надзорен (и) орган (и), освен ако не е уговорено друго.

6.6. Разходи

6.6.1. Всеки от участващите надзорни органи ще заплати собствените си разходи, направени за участието му в съвместната операция, освен ако заинтересованите участници не се договорят за различно споделяне на разходите.

6.7. Разрешаване на спорове

6.7.1. За разрешаване на евентуални незначителни спорове (например евентуални конфликти между длъжностните лица, участващи в съвместната операция, практически или логистични проблеми и т.н.) трябва да бъде определено звено за контакт от всеки участващ надзорен орган. Тези звена за контакт трябва да действат така, че да намерят решение.

6.7.2. Всички участващи надзорни органи ще положат всички усилия за разрешаване на конфликти, които могат да възникнат и да изложат съвместната операция на риск по отношение на ефективността. В случай на конфликт, в резултат на който съвместната операция е невъзможна, участващите надзорни органи могат да използват механизмите, предвидени в Регламент (ЕС) 2016/679, като например чл. 64, § 2 и чл. 66.

6.8. Оттегляне на участващ надзорен орган от съвместната операция

6.8.1. Всеки от участващите надзорни органи може да реши да прекрати участието си в съвместната операция. За да бъде в сила оттеглянето, надзорния орган ще уведоми писмено останалите участници, като предостави правни и/или фактически мотиви или аргументи за своето оттегляне и достатъчно време преди това и ще си сътрудничи по лоялен начин, за да сведе до минимум последиците от оттеглянето му от съвместната операция.

6.8.2. Оттеглянето на водещия надзорен орган ще прекрати съвместната операция, тъй като засегнатите надзорни органи няма да могат да продължат служебно. Поради тази причина това оттегляне трябва да бъде на извънредна основа и трябва да се

основава на загубата на компетентност като водещ надзорен орган или на прекратяването на причините, довели до организирането на съвместната операция.

7. Приложение: План за действие за съвместна операция

Съществуването на някои специфични елементи и, където е уместно, нивото на подробност, ще зависи от всяка съвместна операция и може да бъде актуализирано по време на изпълнението на съвместната операция. Участващите надзорни органи трябва проактивно да положат всички усилия да изградят реалистичен и ефективен план за действие, като се вземат предвид ограничения като например ресурси, време, разходи и т.н.

Планът за действие за съвместна операция може да съдържа:

- **Контекст, цел и обхват на съвместната операция**
- **Участващи надзорни органи**
- **Дати (или ключов етап) на началото и края на съвместната операция.**
- **Персонал, участващ в съвместната операция:**
  - **Лица с пряко участие в съвместната операция: идентификация, роли, умения и отговорности**
  - **Лица, упълномощени да участват във възможни проверки или одити Звена за контакт за разрешаване на спорове.**
- **Планиране на съвместна операция:**
  - **Календари**
  - **Дейности**
  - **Ключови етапи**
  - **Продукти**
  - **Други**
- **Разбивка на разходите**
- **Поверителност и прозрачност**

8. Приложение: Диаграми на съвместни операции

- Сценарий: Съвместна операция с участието на водещ надзорен орган
- Сценарий: Съвместна операция между надзорни органи (без водещ надзорен орган)

Б. Съвместни проверки в Република България, извършвани от дирекция „ППН“, отдел „КАНП“

1. Неприсъствени действия / Планиране / Предварителна подготовка

1.1. когато АЛД/ОЛД е установен в няколко държави членки или има вероятност от операции по обработване на данни да засегнат съществено значителен брой субекти на данни в повече от една държава членка, надзорният орган на всяка държава има право да участва в съвместни операции;

1.2. когато КЗЛД е компетентен орган, отправя покана за съвместна операция и осъществява кореспонденция със съответния/те надзорен/и орган/и по отношение на определените от негова/тяхна страна представители за участие в операцията (членове или персонал на другия/другите надзорен/и орган/и). Кореспонденцията се осъществява от служителите на отдел „КАНП“;

1.3. официалният език при провеждане на съвместни операции в Република България, при които КЗЛД е компетентен орган, е българският;

1.4. при постъпило искане или констатирана необходимост от съвместна операция, отдел „КАНП“ изготвя докладна записка с предложение за евентуално участие на КЗЛД;

1.5. приемане на Решение на КЗЛД за извършване на проверка с определяне на предмета, обхвата и целите на проверката, включително привличане на външен експерт и преводач (при необходимост):

1.5.1. външният експерт и преводачът задължително подписват декларация за неразкриване и неразгласяване на факти и обстоятелства, станали им известни при и по повод извършваната проверка;

1.6. издаване на заповед за проверка с определяне на екипа за проверка, в т.ч. представителите на другия/другите надзорен/и орган/и – два оригинала, с приложен заверен превод на документ, издаден от другия/другите надзорен/и орган/и, в който са определени неговите/техните представители и задачите, които им е поставил;

1.7. предварителна работна среща на служителите на отдел „КАНП“ и представителите на другия/другите надзорен/и орган/и за обсъждане на конкретния казус и въпросите, които следва да се засегнат по време на съвместната операция;

1.8. проучване на приложимото към казуса законодателство и Насоките на Европейския комитет по защита на данните;

1.9. проучване на приложима към казуса практика – на КЗЛД, на Съда на Европейския съюз;

1.10. предварително проучване на АЛД/ОЛД, в т.ч. има ли подадени жалби, сигнали, уведомления в КЗЛД и откази от съдействие, издадените АУАН и НП;

1.11. справки в публични бази данни;

1.12. справки в интернет страници;

1.13. телефонни разговори;

1.14. електронни съобщения;

1.15. изискване на становище/становища;

1.16. изпращане на уведомително писмо до АЛД/ОЛД за проверката с приложен въпросник, включително и по електронен път. В писмото изрично се посочва, че ще бъде извършена съвместна операция с представители на друг/и надзорен/и орган/и.

2. Проверка на място

2.1. легитимиране на проверяващия екип със служебни карти;

2.2. легитимация на представляващия АЛД/ОЛД;

2.3. връчване на заповедта на председателя на КЗЛД за извършване на проверката – връчва се оригинал на заповедта, като на екземпляра на проверяващия екип АЛД/ОЛД или упълномощеното от него лице собственоръчно написва текст, че е получил копие от заповедта за проверка, датата, трите си имена и подпис (за юридическите лица – печат, при възможност);

2.4. изясняване на факти и обстоятелства по отношение на казуса:

2.4.1. проверка за законосъобразно обработване на лични данни съобразно предмета на казуса и задачата на проверката;

2.4.2. предаване на лични данни на трети държави или международни организации (чл. 44–50 от Регламент (ЕС) 2016/679) на кои, основанието и начин на предаване, категории лични данни, технически и организационни мерки за защита;

2.4.3. обмен на лични данни с български институции – на кои, основанието и начин на предаване, категории лични данни, технически и организационни мерки за защита;

2.4.4. наличие на одити по отношение спазването на Наредбата за минимални изисквания за мрежова и информационна сигурност и ISO 27701 (ако е относимо към предмета на казуса);

2.4.5. проверка на сигурността и сертифициране на информационните системи, обработващи лични данни (ако е относимо към предмета на казуса);

2.4.6. наличие на сертификати за информационна сигурност и за защита на личните данни (ако е относимо към предмета на казуса).

2.5. присъединил ли се е АЛД/ОЛД към одобрен кодекс за поведение (ако е относимо към предмета на казуса);

2.6. събиране на доказателства за всеки установен факт – документи на хартиен и/или електронен носител (в т.ч. направения анализ на риска и определяне на нивото на въздействие, правила, процедури, становища, екранни разпечатки и др.), като задължително АЛД/ОЛД предоставя заверени копия на сключени договори с физически или юридически лица, касаещи обработването на лични данни;

2.7. изготвяне на констативен протокол по време на проверката, екземпляр се връчва на АЛД/ОЛД, подписан от всички членове на проверяващия екип;

2.8. изготвяне на приемо-предавателен протокол със заверени копия на документи и предоставени доказателства от АЛД/ОЛД, подписан от всички членове на проверяващия екип, екземпляр се връчва на АЛД/ОЛД;

2.9. указване на срок за предоставяне на допълнителни документи (при необходимост).

3. Приключване на проверката

3.1. анализ на събраните в хода на проверката документи, в т.ч. Насоките на Европейския комитет по защита на данните и решенията на Съда на Европейския съюз, приложими към казуса;

3.2. анализ на сключените договори с физически или юридически лица и наличието на клаузи, регламентиращи обработването на личните данни;

3.3. провеждане на работна среща на служителите на отдел „КАНП“ и представителите на другия/те надзорен/и орган/и, работещи по преписката, за обсъждане на направените констатации по време на проверката на място и анализа на събраните документи и доказателства. Срещата може да бъде осъществена чрез дистанционна комуникация / конферентна връзка;

3.4. изготвяне на констативен акт, подписан от всички членове на проверяващия екип, в т.ч. представителите на друг/и надзорен/и орган/и, като задължително включва мнение и предложения на проверяващия екип;

3.5. констативният акт се завежда в деловодната система, ведно с приложените в оригинал документи и доказателства, като задължително съдържа:

3.5.1. предложение за приемане при липса на нарушение;

3.5.2. предложение за издаване на корективна мярка по чл. 58, § 2 от Регламент (ЕС) 2016/679;

3.5.3 при установяване на административно нарушение – предложение за налагане на санкция на отделните субекти, обект на проверката, стартиране на производство по ЗАНН със съставяне и връчване на АУАН.

3.6. изготвеният констативен акт се внася за разглеждане и приемане на заседание на КЗЛД.

4. Последващи действия на КЗЛД

4.1. приемане с решение на изготвения констативен акт;

4.2. изготвяне на писмо до АЛД/ОЛД с констатации от проверката (когато няма наложена корективна мярка);

4.3. при издаване на корективна мярка по чл. 58, § 2, б. „г“ от Регламент (ЕС) 2016/679:

4.3.1. Решение на КЗЛД − диспозитивът на Решението задължително съдържа издадената корективна мярка (разпореждане), срок за нейното изпълнение, срок за представяне на доказателства за изпълнението му от АЛД/ОЛД, информация за административно-наказателната отговорност, която носи АЛД/ОЛД в случай, че не го изпълни или не изпрати доказателства за изпълнението му в указания срок, както и за възможността за обжалване пред съответния съд;

4.3.2. Решението се връчва на съответните АЛД/ОЛД;

4.3.3. след изтичане на 14-дневен срок влиза в сила и подлежи на изпълнение, ако ответната страна не оспорва Решението;

4.3.4. предоставяне на писмени доказателства от АЛД/ОЛД за изпълнение на корективната мярка и докладване на заседание на КЗЛД;

4.3.5. ако в указания срок АЛД/ОЛД не представи доказателства за изпълнение на корективната мярка:

а) изпраща се напомнително писмо с обратна разписка с указан 7-дневен срок, в който АЛД/ОЛД следва да предостави доказателства и/или становище за изпълнение на решението на КЗЛД и нейните разпореждания, както и информация за административно-наказателната отговорност, която носи АЛД/ОЛД в случай, че не го изпълни;

б) при изпълнение на указаното с писмото, се изготвя докладна записка до КЗЛД с предложение за приемане;

в) в случай на неизпълнение на указаното с писмото, се изготвя докладна записка до КЗЛД с предложение за налагане на административна санкцияпо реда на чл. 83, § 6 от Регламент (ЕС) 2016/679 и чл. 84 от ЗЗЛД, която се докладва на КЗЛД;

г) вземане на Решение на КЗЛД.

4.3.6. изготвяне на уведомително писмо от служителите на отдел „КАНП“ до другия/другите надзорен/и орган/и, съдържащо информация за констатациите, направени по време на съвместната операция, решението на КЗЛД, издадените разпореждания и сроковете за тяхното изпълнение, наложените санкции;

4.3.7. издадените констативни актове, АУАН, НП и решенията за корективни мерки по чл. 58, § 2 от Регламент (ЕС) 2016/679 се вписват и съхраняват в съответния регистър.

III. ПРОВЕРКИ ПРИ ВИСОК ОБЩЕСТВЕН ИНТЕРЕС / САМОСЕЗИРАНЕ НА КЗЛД – ДИРЕКЦИЯ „ППН“, ОТДЕЛ „КАНП“

1. Неприсъствени действия / Планиране / Предварителна подготовка

1.1. приемане на решение на КЗЛД за извършване на проверка с определяне на предмета, обхвата и целите на проверката, включително привличане на външен експерт (при необходимост);

1.2. издаване на заповед за проверка с определяне на екипа за проверка –два оригинала;

1.3. проучване на приложимото към казуса законодателство и Насоките на Европейския комитет по защита на данните;

1.4. проучване на приложима към казуса практика – на КЗЛД, на Съда на Европейския съюз;

1.5. предварително проучване на АЛД/ОЛД, в т.ч. има ли подадени жалби, сигнали, уведомления в КЗЛД и откази от съдействие, издадените АУАН и НП;

1.6. справки публични бази данни;

1.7. справки интернет страници;

1.8. телефонни разговори;

1.9. електронни съобщения;

1.10. изискване на становище/становища;

1.11. изпращане на уведомително писмо до АЛД за проверката с приложен въпросник, включително и по електронен път.

2. Проверка на място

2.1. легитимиране на проверяващия екип със служебни карти;

2.2. легитимация на представляващия АЛД/ОЛД;

2.3. връчване на заповедта на председателя на КЗЛД за извършване на проверката – връчва се оригинал на заповедта, като на екземпляра на проверяващия екип АЛД/ОЛД или упълномощеното от него лице собственоръчно написва текст, че е получил копие от заповедта за проверка, датата, трите си имена и подпис (за юридическите лица – печат, при възможност);

2.4. задължителна проверка и събиране на доказателства относно:

2.4.1. спазване принципите за законосъобразно обработване на лични данни (чл. 5, 6 от Регламент (ЕС) 2016/679);

2.4.2. условията за даване на съгласие (чл. 7 от Регламент (ЕС) 2016/679);

2.4.3. условията, приложими за съгласието на дете във връзка с услугите на информационното общество (чл. 8 от Регламент (ЕС) 2016/679);

2.4.4. обработването на специални категории лични данни (чл. 9 от Регламент (ЕС) 2016/679);

2.4.5. предприетите от АЛД/ОЛД действия за информиране на физическите лица за целите на обработване на личните им данни и упражняването на техните права съгласно чл. 15–22 от Регламент (ЕС) 2016/679;

2.4.6. предаване на лични данни на трети държави или международни организации (чл. 44–50 от Регламент (ЕС) 2016/679) на кои, основанието и начин на предаване, категории лични данни, технически и организационни мерки за защита;

2.4.7. обмен на лични данни с български институции – на кои, основанието и начин на предаване, категории лични данни, технически и организационни мерки за защита;

2.4.8. предприетите технически и организационни мерки за защита на личните данни;

2.4.9. наличие на одити по отношение спазването на Наредбата за минимални изисквания за мрежова и информационна сигурност и ISO 27701;

2.4.10. проверка на сигурността и сертифициране на информационните системи, обработващи лични данни;

2.4.11. наличие на сертификати за информационна сигурност и за защита на личните данни;

2.4.12. присъединил ли се е АЛД/ОЛД към одобрен кодекс за поведение.

2.5. събиране на доказателства за всеки установен факт – документи на хартиен и/или електронен носител (в т.ч. направения анализ на риска и определяне на нивото на въздействие, правила, процедури, становища, екранни разпечатки и др.), като

задължително АЛД/ОЛД предоставя заверени копия на сключени договори с физически или юридически лица, касаещи обработването на лични данни;

2.6. изготвяне на констативен протокол по време на проверката, екземпляр се връчва на АЛД/ОЛД;

2.7. изготвяне на приемо-предавателен протокол със заверени копия на документи и предоставени доказателства от АЛД/ОЛД, екземпляр се връчва на АЛД/ОЛД;

2.8. указване на срок за предоставяне на допълнителни документи (при необходимост).

3. Приключване на проверката

3.1. анализ на събраните в хода на проверката документи, в т.ч. Насоките на Европейския комитет по защита на данните и решенията на Съда на Европейския съюз, приложими към казуса;

3.2. анализ на сключените договори с физически или юридически лица и наличието на клаузи, регламентиращи обработването на личните данни;

3.3. изготвяне на констативен акт и завеждането му в деловодната система, ведно с приложените в оригинал документи и доказателства, като задължително включва мнение и предложения на проверяващия екип:

3.3.1. предложение за приемане при липса на нарушение;

3.3.2. предложение за издаване на корективна мярка по чл. 58, § 2 от Регламент (ЕС) 2016/679;

3.3.3. при установяване на административно нарушение – предложение за налагане на санкция на отделните субекти, обект на проверката, стартиране на производство по ЗАНН със съставяне и връчване на АУАН.

3.4. изготвеният констативен акт се внася за разглеждане и приемане на заседание на КЗЛД.

4. Последващи действия на КЗЛД

4.1. приемане с решение на изготвения констативен акт;

4.2. изготвяне на писмо до АЛД/ОЛД с констатации от проверката (когато няма наложена корективна мярка);

4.3. при издаване на корективна мярка по чл. 58, § 2, б. „г“ от Регламент (ЕС) 2016/679:

4.3.1. Решение на КЗЛД - диспозитивът на Решението задължително съдържа издадената корективна мярка (разпореждане), срок за нейното изпълнение, срок за

представяне на доказателства за изпълнението му от АЛД/ОЛД, информация за административно-наказателната отговорност, която носи АЛД/ОЛД в случай, че не го изпълни или не изпрати доказателства за изпълнението му в указания срок, както и за възможността за обжалване пред съответния съд;

4.3.2. Решението се връчва на съответните АЛД/ОЛД;

4.3.3. след изтичане на 14-дневен срок влиза в сила и подлежи на изпълнение, ако ответната страна не оспорва Решението;

4.3.4. предоставяне на писмени доказателства от АЛД/ОЛД за изпълнение на корективната мярка и докладване на заседание на КЗЛД;

4.3.5. ако в указания срок АЛД/ОЛД не представи доказателства за изпълнение на корективната мярка:

а) изпраща се напомнително писмо с обратна разписка с указан 7-дневен срок, в който АЛД/ОЛД следва да предостави доказателства и/или становище за изпълнение на решението на КЗЛД и нейните разпореждания, както и информация за административно-наказателната отговорност, която носи АЛД/ОЛД в случай, че не го изпълни;

б) при изпълнение на указаното с писмото, се изготвя докладна записка до КЗЛД с предложение за приемане;

в) в случай на неизпълнение на указаното с писмото, се изготвя докладна записка до КЗЛД с предложение за налагане на административна санкцияпо реда на чл. 83, § 6 от Регламент (ЕС) 2016/679 и чл. 84 от ЗЗЛД, която се докладва на КЗЛД;

г) вземане на Решение на КЗЛД.

4.4. издадените констативни актове се присъединяват към преписката;

4.5. издадените АУАН, НП и решенията за корективни мерки по чл. 58, § 2 от Регламент (ЕС) 2016/679 се вписват и съхраняват в съответния регистър.

IV. ПРОВЕРКИ ПО ЖАЛБИ СЛЕД РЕШЕНИЕ НА КЗЛД – ДИРЕКЦИЯ „ППН“, ОТДЕЛ „КАНП“

Спазва се принципът „Който стартира процедурата, той я приключва“

1. Неприсъствени действия / Планиране / Предварителна подготовка

1.1. приемане на решение на КЗЛД за извършване на проверка с определяне на предмета, обхвата и целите на проверката, в т.ч. при необходимост от привличане на външен експерт;

1.2. издаване на заповед за проверка с определяне на екипа за проверка – два оригинала;

1.3. проучване на приложимото към казуса законодателство и Насоките на Европейския комитет по защита на данните (анализа го правят служителите на „ППППП” в становището по жалбата);

1.4. проучване на приложима към казуса практика – на КЗЛД, на Съда на Европейския съюз (анализа го правят служителите на „ППППП” в становището по жалбата);

1.5. предварително проучване на АЛД/ОЛД, в т.ч. има ли подадени за него жалби, сигнали, уведомления в КЗЛД и наличие на откази от съдействие, издадените АУАН и НП (анализа го правят служителите на „ППППП” в становището по жалбата);

1.6 уведомяване на АЛД/ОЛД за проверката:

1.6.1. телефонни разговори;

1.6.2. електронни съобщения;

1.6.3. изпращане на уведомително писмо с въпросник (при необходимост), включително и по електронен път.

2. Проверка на място

2.1. легитимиране на проверяващия екип със служебни карти;

2.2. легитимация на представляващия АЛД/ОЛД;

2.3. връчване на заповедта на председателя на КЗЛД за извършване на проверката – връчва се оригинал на заповедта, като на екземпляра на проверяващия екип АЛД/ОЛД или упълномощеното от него лице собственоръчно написва текст, че е получил копие от заповедта за проверка, датата, трите си имена и подпис (за юридическите лица – печат, при възможност);

2.4. проверка за законосъобразно обработване на лични данни, съобразно предмета на жалбата и задачата на проверката;

2.5. наличие на одити по отношение спазването на Наредбата за минимални изисквания за мрежова и информационна сигурност и ISO 27701 (ако е относимо към предмета на жалбата);

2.6. проверка на сигурността и сертифициране на информационните системи, обработващи лични данни (ако е относимо към предмета на жалбата);

2.7. наличие на сертификати за информационна сигурност и за защита на личните данни (ако е относимо към предмета на жалбата);

2.8. предаване на лични данни на трети държави или международни организации (чл. 44–50 от Регламент (ЕС) 2016/679) на кои, основанието и начин на предаване, категории лични данни, технически и организационни мерки за защита (ако е относимо към предмета на жалбата);

2.9. обмен на лични данни с български институции – на кои, основанието и начин на предаване, категории лични данни, технически и организационни мерки за защита (ако е относимо към предмета на жалбата);

2.10. присъединил ли се е АЛД/ОЛД към одобрен кодекс за поведение (ако е относимо към предмета на жалбата);

2.11. събиране на доказателства за всеки установен факт – документи на хартиен и/или електронен носител (в т.ч. направения анализ на риска и определяне на нивото на въздействие, правила, процедури, становища, екранни разпечатки и др.), като задължително АЛД/ОЛД предоставя заверени копия на сключени договори с физически или юридически лица, касаещи обработването на лични данни;

2.12. изготвяне на констативен протокол по време на проверката, екземпляр се връчва на АЛД/ОЛД;

2.13. изготвяне на приемо-предавателен протокол със заверени копия на документи и предоставени доказателства от АЛД/ОЛД, екземпляр се връчва на АЛД/ОЛД;

2.14. указване на срок за предоставяне на допълнителни документи (при необходимост).

3. Приключване на проверката

3.1. изготвяне на констативен акт (не включва мнение и предложения на проверяващия екип) и завеждането му в деловодната система, ведно с приложените в оригинал документи и доказателства;

3.2. докладване на констативния акт на заседание на КЗЛД за приобщаването му към доказателствата към съответната жалба;

3.3. сканираният в деловодната система констативен акт, ведно с приложените документи и доказателства, се резолира за отдел „ПППП” за изготвяне на становище по жалбата.

V. ПРОВЕРКИ ПО СИГНАЛИ – ДИРЕКЦИЯ „ППН“, ОТДЕЛ „КАНП“

1. Проверка само по документи

1.1. входиране на сигнал в деловодството на КЗЛД;

1.2. определяне на служител / екип от служители за разглеждането на сигнала;

1.3. проучване на нормативната уредба поконкретния казус;

1.4. проучване на АЛД/ОЛД – седалище и адрес на управление, предмета на дейност и др.;

1.5. справки в публични бази данни;

1.6. справки в интернет страници;

1.7. телефонни разговори;

1.8. електронни съобщения;

1.9. изискване на становище/становища;

1.10. искане на становище/становища (при необходимост);

1.11. изготвяне на отговор до сигналоподателя, без да се предприемат последващи действия;

1.12. сигналът да се препрати по компетентност на друг орган/органи;

1.13. в зависимост от казуса на сигнала и събраните документи може:

1.13.1. да се изготви докладна записка, която да се докладва на КЗЛД със съответните предложения на служителя, разглеждащ сигнала. Докладната може да съдържа предложения за преквалифицирането на сигнала в жалба, за издаване на корективна мярка по чл. 58, § 2 от Регламент (ЕС) 2016/679, за препращане на сигнала на друг компетентен орган, включително по Информационната система на вътрешния пазар и др.;

1.13.2. да се изготви АУАН/НП само на база на събрани документи, без проверка на място, като задължително служителите на КЗЛД следва да предприемат действия за потвърждение на фактите и обстоятелствата, съдържащи се в документите и събирането на допълнителни писмени материали, с оглед упражняването на правомощията на КЗЛД;

1.14. при получаване на документи, изпратени по компетентност на КЗЛД от Прокуратурата на Република България / МВР и други органи:

1.14.1. препращане по компетентност на друг орган / органи;

1.14.2. издаване на корективна мяркапо чл. 58, § 2 от Регламент (ЕС) 2016/679;

1.14.3. стартиране на процедура по ЗАНН със съставяне на АУАН по документи, като служителите на КЗЛД следва задължително да предприемат действия за потвърждение на фактите и обстоятелствата, съдържащи се в документите и събирането на допълнителни писмени материали, с оглед упражняването на правомощията на КЗЛД.

1.15. изготвяне на отговор до сигналоподателя, съдържащ информация за предприетите от КЗЛД действия, с препращане към друг орган / издаване на корективна мярка / налагане на санкция.

2. Проверка на място на АЛД/ОЛД

2.1. Неприсъствени действия / Планиране / Предварителна подготовка:

2.1.1. издаване на заповед за проверка с определяне на екипа за проверка, предмета, обхвата и целите на проверката, включително привличане на външен експерт(при необходимост) –два оригинала;

2.1.2. проучване на приложимото към казуса законодателство и Насоките на Европейския комитет по защита на данните;

2.1.3. проучване на приложима към казуса практика – на КЗЛД, на Съда на Европейския съюз;

2.1.4. предварително проучване на АЛД/ОЛД, в т.ч. има ли подадени жалби, сигнали, уведомления в КЗЛД и откази от съдействие, издадените АУАН и НП;

2.1.5. справки в публични бази данни;

2.1.6. справки в интернет страници;

2.1.7. телефонни разговори;

2.1.8. електронни съобщения;

2.1.9. изискване на становище/становища;

2.1.10. изпращане на уведомително писмо с въпросник (при необходимост), включително и по електронен път.

2.2. Проверка на място в седалището/обект на АЛД/ОЛД:

2.2.1. легитимиране на проверяващия екип със служебни карти;

2.2.2. легитимация на представляващия АЛД/ОЛД;

2.2.3. връчване на заповедта на председателя на КЗЛД за извършване на проверката – връчва се оригинал на заповедта, като на екземпляра на проверяващия екип АЛД/ОЛД или упълномощеното от него лице собственоръчно написва текст, че е получил копие от заповедта за проверка, датата, трите си имена и подпис (за юридическите лица – печат, при възможност);

2.2.4. изясняване на факти и обстоятелства по отношение на получения сигнал:

а) проверка за законосъобразно обработване на лични данни съобразно предмета на сигнала и задачата на проверката;

б) предаване на лични данни на трети държави или международни организации (чл. 44–50 от Регламент (ЕС) 2016/679) – на кои, основанието и начин на предаване, категории лични данни, технически и организационни мерки за защита (ако е относимо към предмета на сигнала);

в) обмен на лични данни с български институции – на кои, основанието и начин на предаване, категории лични данни, технически и организационни мерки за защита (ако е относимо към предмета на сигнала);

г) наличие на одити по отношение спазването на Наредбата за минимални изисквания за мрежова и информационна сигурност и ISO 27701 (ако е относимо към предмета на сигнала);

д) проверка на сигурността и сертифициране на информационните системи, обработващи лични данни (ако е относимо към предмета на сигнала);

е) наличие на сертификати за информационна сигурност и за защита на личните данни (ако е относимо към предмета на сигнала);

ж) присъединил ли се е АЛД/ОЛД към одобрен кодекс за поведение (ако е относимо към предмета на сигнала).

2.2.5. събиране на доказателства за всеки установен факт – документи на хартиен и/или електронен носител (в т.ч. направения анализ на риска и определяне на нивото на въздействие, правила, процедури, становища, екранни разпечатки и др.), като задължително АЛД/ОЛД предоставя заверени копия на сключени договори с физически или юридически лица, касаещи обработването на лични данни;

2.2.6. изготвяне на констативен протокол по време на проверката, екземпляр се връчва на АЛД/ОЛД;

2.2.7. изготвяне на приемо-предавателен протокол със заверени копия на документи и предоставени доказателства от АЛД/ОЛД, екземпляр се връчва на АЛД/ОЛД;

2.2.8. указване на срок за предоставяне на допълнителни документи (при необходимост).

3. Приключване на проверката

3.1. анализ на събраните в хода на проверката документи, в т.ч. Насоките на Европейския комитет по защита на данните и решенията на Съда на Европейския съюз, приложими към казуса;

3.2. анализ на сключените договори с физически или юридически лица и наличието на клаузи, регламентиращи обработването на личните данни;

3.3. изготвяне на констативен акт и завеждането му в деловодната система, ведно с приложените в оригинал документи и доказателства, като задължително включва мнение и предложения на проверяващия екип:

3.3.1. предложение за приемане при липса на нарушение;

3.3.2. предложение за издаване на корективна мярка по чл. 58, § 2 от Регламент (ЕС) 2016/679;

3.3.3. при установяване на административно нарушение – предложение за налагане на санкция на АЛД/ОЛД, със стартиране на производство по ЗАНН със съставяне и връчване на АУАН;

3.4. изготвеният констативен акт се внася за разглеждане и приемане на заседание на КЗЛД.

4. Последващи действия на КЗЛД

4.1. приемане с Решение на изготвения констативен акт;

4.2. изготвяне на писмо до АЛД/ОЛД с констатации от проверката (когато няма наложена корективна мярка);

4.3. при издаване на корективна мярка по чл. 58, § 2, б. „г“ от Регламент (ЕС) 2016/679:

4.3.1. Решение на КЗЛД – диспозитивът на Решението задължително съдържа издадената корективна мярка (разпореждане), срок за нейното изпълнение, срок за представяне на доказателства за изпълнението му от АЛД/ОЛД, информация за административно-наказателната отговорност, която носи АЛД/ОЛД в случай, че не го изпълни или не изпрати доказателства за изпълнението му в указания срок, както и за възможността за обжалване пред съответния съд;

4.3.2. Решението се връчва на съответните АЛД/ОЛД;

4.3.3. след изтичане на 14-дневен срок влиза в сила и подлежи на изпълнение, ако ответната страна не оспорва Решението;

4.3.4. предоставяне на писмени доказателства от АЛД/ОЛД за изпълнение на коректиавната мярка и докладване на заседание на КЗЛД;

4.3.5. ако в указания срок АЛД/ОЛД не представи доказателства за изпълнение на коректиавната мярка:

а) изпраща се напомнително писмо с обратна разписка с указан 7-дневен срок, в който АЛД/ОЛД следва да предостави доказателства и/или становище за изпълнение на решението на КЗЛД и нейните разпореждания, както и информация за

административно-наказателната отговорност, която носи АЛД/ОЛД в случай, че не го изпълни;

б) при изпълнение на указаното с писмото, се изготвя докладна записка до КЗЛД с предложение за приемане;

в) в случай на неизпълнение на указаното с писмото, се изготвя докладна записка до КЗЛД с предложение за налагане на административна санкция по реда на чл. 83, § 6 от Регламент (ЕС) 2016/679 и чл. 84 от ЗЗЛД, която се докладва на КЗЛД;

г) вземане на Решение на КЗЛД.

4.4. издадените констативни актове се присъединяват към преписката;

4.5. оздадените АУАН, НП и решенията за корективни мерки по чл. 58, § 2 от Регламент (ЕС) 2016/679 се вписват и съхраняват в съответния регистър.

VI. ПРОВЕРКИ ПРИ УВЕДОМЛЕНИЯ ПО чл. 33 ОТ РЕГЛАМЕНТ (ЕС) 2016/679 И чл. 67 ОТ ЗЗЛД– ДИРЕКЦИЯ „ПАИКД“

Спазва се принципът „Който стартира процедурата, той я приключва“

А. Предварителен анализ на уведомлението от дирекция „ПАИКД“

1. Неприсъствени действия / Планиране / Предварителна подготовка

1.1. входиране на уведомление в деловодството на КЗЛД (по образец, одобрен от КЗЛД, когато е приложимо);

1.2. вписване в регистъра на уведомленията;

1.3. определяне на служител / екип от служители за разглеждането на уведомлението;

1.4. анализ на подаденото уведомление – проверка отговаря ли уведомлението на изискванията на чл. 33, § 3 от Регламент (ЕС) 2016/679. Извършва се в 14-дневен срок и включва:

1.4.1. идентификация на АЛД/ОЛД, подал уведомлението – седалище и адрес на управление, предмета на дейност и др.;

1.4.2. проверка дали АЛД/ОЛД е определил ДЛЗД и уведомена ли е КЗЛД за него, съответно предоставени ли са координати за връзка с него;

1.4.3. качество на КЗЛД спрямо АЛД/ОЛД (водещ надзорен орган, засегнат надзорен орган или компетентен орган по чл. 56, § 2 от Регламент (ЕС) 2016/679):

а) в случай, че КЗЛД е засегнат или компетентен орган, служителят/ите на дирекция „ПАИКД“ изготвят докладна записка, която се докладва на заседание на КЗЛД:

– установяване на факти и обстоятелства по подаденото уведомление;

– срок от извършване и узнаване на нарушението;

– описание на естеството на нарушението;

– евентуални последици от нарушението;

– поредност на нарушението;

– категории и брой на засегнатите субекти на данни;

– преценка на тежестта на последствията върху субектите на данни;

– категории и брой на засегнати лични данни;

– описание на предприетите или предложените от АЛД/ОЛД мерки за справяне с нарушението;

– информиране на субектите на данни, засегнати от нарушението;

– в случай, че се констатира непълнота на данните по чл. 33, § 3 от Регламент (ЕС) 2016/679, без забавяне, се осъществява контакт с АЛД/ОЛД, чрез предоставените от него координати за връзка и/или се изпраща писмо (в т.ч. по електронна поща) да предостави необходимата информация, като му се указва 3-дневен срок;

б) приемане на решение на КЗЛД за нейното конституиране като засегнат или компетентен орган;

в) след приемането му, съответната информация незабавно се качва в Информационната система на вътрешния пазар;

г) при възникнал спор за компетентност, служителят/ите на дирекция „ПАИКД“ изготвят докладна записка с мотивирано предложение до КЗЛД за отнасяне на спора до Европейския комитет за защита на данните по реда на чл. 65 или чл. 66 от Регламент (ЕС) 2016/679 и в съответствие с Насоки за определяне на водещ надзорен орган на администратор или обработващ личните данни, приети от Европейския комитет по защита на данните.

1.5. проучване и анализ на приложимото към казуса законодателство и Насоките на Европейския комитет по защита на данните (в т.ч. Насоки относно уведомяването за нарушения на сигурността на личните данни съгласно Регламент (ЕС) 2016/679, Решения на Съда на ЕС, ако са приложими към уведомлението);

1.6. проучване и анализ на приложима към казуса практика – на КЗЛД, на Съда на Европейския съюз;

1.7. предварително проучване на АЛД/ОЛД, в т.ч. има ли подадени жалби, сигнали, уведомления в КЗЛД и откази от съдействие, издадените АУАН и НП;

1.8. проверка за наличието на жалби, депозирани чрез Информационната система на вътрешния пазар, когато се споменава администратор, установен в България и обработващ данни на граждани от други държави членки;

1.9. справки в публични бази данни;

1.10. справки в интернет страници;

1.11. телефонни разговори;

1.12. електронни съобщения.

2. Докладване на КЗЛД от дирекция „ПАИКД“

2.1. въз основа на направения анализ и Методиката за определяне нивото на риска при нарушение сигурността на данните (Приложение № 1 към настоящата Инструкция), служителя/ите на „ПАИКД“ изготвя/т докладна записка до КЗЛД, като определят съответно ниво на риск на нарушението, съобразно одобрени от КЗЛД критерии, а именно „ниско ниво на риск“, „средно ниво на риск“, „високо ниво на риск“;

2.2. докладната записка се внася на заседание на КЗЛД, с предложение, както следва:

2.2.1. при „ниско ниво на риск“ – уведомлението да се приеме за сведение;

2.2.2. при „средно ниво на риск“ – да се извърши проверка по документи от дирекция „ПАИКД“;

2.2.3 при „високо ниво на риск“ – да се извърши проверка на място от дирекция „ППН“.

2.3. приемане на Решение на КЗЛД, както следва:

2.3.1. „ниско ниво на риск“ – уведомлението се приема за сведение, за което се уведомява АЛД/ОЛД;

2.3.2. „средно ниво на риск“ – да се извърши проверка по документи от дирекция „ПАИКД“;

2.3.3. „високо ниво на риск“ – да се извърши проверка на място от дирекция „ППН“, отдел „КАНП“, с определяне на предмета, обхвата и целите на проверката, в т.ч. необходимост от привличане на външен експерт.

Б. Проверки по документи при „средно ниво на риск“ от дирекция „ПАИКД“

1. Неприсъствени действия / Планиране / Предварителна подготовка от дирекция „ПАИКД“

1.1. изискване на становище/становища (при необходимост);

1.2. изпращане на уведомително писмо с въпросник, вкл. и по електронен път;

1.3. проверка за законосъобразно обработване на лични данни съобразно предмета на уведомлението и задачата на проверката;

1.4. предаване на лични данни на трети държави или международни организации (чл. 44–50 от Регламент (ЕС) 2016/679) – на кои, основанието и начин на предаване, категории лични данни, технически и организационни мерки за защита (ако е относимо към предмета на уведомлението);

1.5. обмен на лични данни с български институции – на кои, основанието и начин на предаване, категории лични данни, технически и организационни мерки за защита (ако е относимо към предмета на уведомлението);

1.6. наличие на одити по отношение спазването на Наредбата за минимални изисквания за мрежова и информационна сигурност и ISO 27701 (ако е относимо към предмета на уведомлението);

1.7. проверка на сигурността и сертифициране на информационните системи, обработващи лични данни (ако е относимо към предмета на уведомлението);

1.8. наличие на сертификати за информационна сигурност и за защита на личните данни (ако е относимо към предмета на уведомлението);

1.9. присъединил ли се е АЛД/ОЛД към одобрен кодекс за поведение (ако е относимо към предмета на уведомлението);

1.10. събиране и анализ на доказателства за всеки установен факт – документи на хартиен и/или електронен носител (в т.ч. направения анализ на риска и определяне на нивото на въздействие, правила, процедури, становища, екранни разпечатки и др.), като задължително от АЛД/ОЛД се изискват заверени копия на сключени договори с физически или юридически лица, касаещи обработването на лични данни.

2. Приключване на проверката

2.1. анализ на събраните в хода на проверката документи, в т.ч. Насоките на Европейския комитет по защита на данните и Решенията на Съда на Европейския съюз, приложими към уведомлението;

2.2. анализ на сключените договори с физически или юридически лица и наличието на клаузи, регламентиращи обработването на личните данни;

2.3. изготвяне на констативен акт и завеждането му в деловодната система, ведно с приложените в оригинал документи и доказателства. Констативният акт задължително включва мнение и предложение на проверяващия екип:

2.3.1. предложение за приемане на констативния акт при установено преодоляване на последствията от нарушението;

2.3.2. предложение за издаване на корективна мярка по чл. 58, § 2 от Регламент (ЕС) 2016/679, в случай, че не са предприети адекватни и подходящи мерки за овладяване на риска;

2.3.3. при установяване на административно нарушение – стартиране на производство по ЗАНН, със съставяне и връчване на АУАН, като задължително служителите на „ПАИКД“ следва да предприемат действия за потвърждение на фактите и обстоятелствата, съдържащи се в документите и събирането на допълнителни писмени материали, с оглед упражняването на правомощията на КЗЛД.

2.4. изготвеният констативен акт се внася за разглеждане и приемане на заседание на КЗЛД.

3. Последващи действия на КЗЛД

3.1. приемане с решение на изготвения констативен акт;

3.2. изготвяне на писмо до АЛД/ОЛД с констатации от проверката (когато няма наложена корективна мярка);

3.3. при издаване на корективна мярка по чл. 58, § 2, б. „г“ от Регламент (ЕС) 2016/679:

3.3.1. Решение на КЗЛД – диспозитивът на Решението задължително съдържа издадената корективна мярка (разпореждане), срок за нейното изпълнение, срок за представяне на доказателства за изпълнението му от АЛД/ОЛД, информация за административно-наказателната отговорност, която носи АЛД/ОЛД в случай, че не го изпълни или не изпрати доказателства за изпълнението му в указания срок, както и за възможността за обжалване пред съответния съд;

3.3.2. Решението се връчва на съответните АЛД/ОЛД;

3.3.3. след изтичане на 14-дневен срок влиза в сила и подлежи на изпълнение, ако ответната страна не оспорва Решението;

3.3.4. предоставяне на писмени доказателства от АЛД/ОЛД за изпълнение на коректиивната мярка и докладване на заседание на КЗЛД;

3.3.5. ако в указания срок АЛД/ОЛД не представи доказателства за изпълнение на коректиивната мярка:

а) изпраща се напомнително писмо с обратна разписка с указан 7-дневен срок, в който АЛД/ОЛД следва да предостави доказателства и/или становище за изпълнение на решението на КЗЛД и нейните разпореждания, както и информация за административно-наказателната отговорност, която носи АЛД/ОЛД в случай, че не го изпълни;

б) при изпълнение на указаното с писмото, се изготвя докладна записка до КЗЛД с предложение за приемане;

в) в случай на неизпълнение на указаното с писмото, се изготвя докладна записка до КЗЛД с предложение за налагане на административна санкцияпо реда на чл. 83, § 6 от Регламент (ЕС) 2016/679 и чл. 84 от ЗЗЛД, която се докладва на КЗЛД;

г) вземане на Решение на КЗЛД;

3.4. издадените констативни актове се присъединяват към преписката;

3.5. издадените АУАН, НП и решенията за корективни мерки по чл. 58, § 2 от Регламент (ЕС) 2016/679 се вписват и съхраняват в съответния регистър.

В. Проверки на място при „високо ниво на риск“ от дирекция „ППН“, отдел „КАНП“

1. Неприсъствени действия / Планиране / Предварителна подготовка от дирекция „ППН“, отдел „КАНП“

1.1. определяне на екип за проверка на място от отдел „КАНП“;

1.2. предварителна работна среща на служителите на дирекция „ПАИКД“ и отдел „КАНП“, работещи по преписката, за обсъждане на подаденото уведомление в 3-дневен срок от докладване на КЗЛД;

1.3. сканираната в деловодната система докладна записка на дирекция „ПАИКД“, ведно с приложените документи и доказателства, събрани в хода на направения от нейните служители анализ, се резолира за отдел „КАНП“ за извършване на проверка на място;

1.4. издаване на заповед за проверка с определяне на екипа за проверка – два оригинала;

1.5. уведомяване на АЛД/ОЛД за проверката:

1.5.1. телефонни разговори;

1.5.2. електронни съобщения;

1.5.3. изпращане на уведомително писмо с въпросник, вкл. и по електронен път.

2. Проверка на място от дирекция „ППН“, отдел „КАНП“

2.1. легитимиране на проверяващия екип със служебни карти;

2.2. легитимация на представляващия АЛД/ОЛД;

2.3. връчване на заповедта на председателя на КЗЛД за извършване на проверката – връчва се оригинал на заповедта, като на екземпляра на проверяващия екип

АЛД/ОЛД или упълномощеното от него лице собственоръчно написва текст, че е получил копие от заповедта за проверка, датата, трите си имена и подпис (за юридическите лица – печат, при възможност);

2.4. проверка за законосъобразно обработване на лични данни съобразно предмета на уведомлението и задачата на проверката;

2.5. задължителна проверка на:

2.5.1. предприети мерки в 72-часов срок;

2.5.2. уведомяване на засегнатите субекти;

2.5.3.предприети мерки за минимализиране на вредите;

2.5.4. има ли постъпили сигнали и жалби до АЛД/ОЛД за конкретното нарушение.

2.6. предаване на лични данни на трети държави или международни организации (чл. 44–50 от Регламент (ЕС) 2016/679) − на кои, основанието и начин на предаване, категории лични данни, технически и организационни мерки за защита (ако е относимо към предмета на уведомлението);

2.7. обмен на лични данни с български институции – на кои, основанието и начин на предаване, категории лични данни, технически и организационни мерки за защита (ако е относимо към предмета на уведомлението);

2.8. наличие на одити по отношение спазването на Наредбата за минимални изисквания за мрежова и информационна сигурност и ISO 27701 (ако е относимо към предмета на уведомлението);

2.9. проверка на сигурността и сертифициране на информационните системи, обработващи лични данни (ако е относимо към предмета на уведомлението);

2.10. наличие на сертификати за информационна сигурност и за защита на личните данни (ако е относимо към предмета на уведомлението);

2.11. присъединил ли се е АЛД/ОЛД към одобрен кодекс за поведение (ако е относимо към предмета на уведомлението);

2.12. събиране на доказателства за всеки установен факт – документи на хартиен и/или електронен носител (в т.ч. направения анализ на риска и определяне на нивото на въздействие, правила, процедури, становища, екранни разпечатки и др.), като задължително АЛД/ОЛД предоставя заверени копия на сключени договори с физически или юридически лица, касаещи обработването на лични данни;

2.13. изготвяне на констативен протокол по време на проверката, екземпляр се връчва на АЛД/ОЛД;

2.14. изготвяне на приемо-предавателен протокол със заверени копия на документи и предоставени доказателства от АЛД/ОЛД, екземпляр се връчва на АЛД/ОЛД;

2.15. указване на срок за предоставяне на допълнителни документи и доказателства (при необходимост).

3. Приключване на проверката на място от дирекция „ППН“, отдел „КАНП“

3.1. изготвяне на констативен акт (не включва мнение и предложения на проверяващия екип) и завеждането му в деловодната система, ведно с приложените в оригинал документи и доказателства;

3.2. при установяване на административно нарушение, в законоустановения срок се стартира производство по ЗАНН със съставяне и връчване на АУАН от служителите на отдел „КАНП“, като това обстоятелство се вписва в констативния акт;

3.3. заключителна работна среща на служителите на „КАНП“ и „ПАИКД“, работещи по преписката, за запознаване с направените констатации по време на проверката на място в 3-дневен срок от изготвяне на констативен акт;

3.4. докладване на констативния акт на заседание на КЗЛД за приобщаването му към съответната преписка на полученото в КЗЛД уведомление;

3.5. сканираният в деловодната система констативен акт, ведно с приложените документи и доказателства, се резолира за „ПАИКД“ за изготвяне на становище.

4. Приключване на проверката от дирекция „ПАИКД“

4.1. дирекция „ПАИКД“ внася на заседание на КЗЛД становище с анализ на цялата събрана в хода на проверката информация с предложение за приемане при установено преодоляване на последствията от нарушението или за приемане на Решение на КЗЛД за налагане на корективни мерки по чл. 58, § 2 от Регламент (ЕС) 2016/679. Становището има следните реквизити: фактическа страна, предприети действия, правен анализ, предложение.

5. Последващи действия на КЗЛД

5.1. приемане с решение на изготвеното от дирекция „ПАИКД“ становище;

5.2. дирекция „ПАИКД“ изготвя проект на решение на КЗЛД;

5.3. изготвяне на писмо от дирекция „ПАИКД“ до АЛД/ОЛД с констатации от проверката (когато няма наложена корективна мярка);

5.4. при издаване на корективна мярка по чл. 58, § 2 от Регламент (ЕС) 2016/679

5.4.1. Решение на КЗЛД - диспозитивът на Решението задължително съдържа издадената корективна мярка (разпореждане), срок за нейното изпълнение, срок за представяне на доказателства за изпълнението му от АЛД/ОЛД, информация за административно-наказателната отговорност, която носи АЛД/ОЛД в случай, че не го изпълни или не изпрати доказателства за изпълнението му в указания срок, както и за възможността за обжалване пред съответния съд (доказателства за изпълнение на корективна мярка по чл. 58, § 2, б. „а“ и „б“ не се изискват);

5.4.2. Решението се връчва на съответните АЛД/ОЛД;

5.4.3. след изтичане на 14-дневен срок влиза в сила и подлежи на изпълнение, ако ответната страна не оспорва Решението;

5.4.4. предоставяне на писмени доказателства от АЛД/ОЛД за изпълнение на коративната мярка и докладване на заседание на КЗЛД;

5.4.5. ако в указания срок АЛД/ОЛД не представи доказателства за изпълнение на коративната мярка:

а) изпраща се напомнително писмо с обратна разписка с указан 7-дневен срок, в който АЛД/ОЛД следва да предостави доказателства и/или становище за изпълнение на решението на КЗЛД и нейните разпореждания, както и информация за административно-наказателната отговорност, която носи АЛД/ОЛД в случай, че не го изпълни;

б) при изпълнение на указаното с писмото, се изготвя докладна записка до КЗЛД с предложение за приемане;

в) в случай на неизпълнение на указаното с писмото, се изготвя докладна записка до КЗЛД с предложение за налагане на административна санкция по реда на чл. 83, § 6 от Регламент (ЕС) 2016/679 и чл. 84 от ЗЗЛД, която се докладва на КЗЛД;

г) вземане на Решение на КЗЛД.

5.5. издадените констативни актове се присъединяват към преписката;

5.6. издадените АУАН, НП и решенията за коративни мерки по чл. 58, § 2 от Регламент (ЕС) 2016/679 се вписват и съхраняват в съответния регистър.

VII. ПРЕДВАРИТЕЛНИ КОНСУЛТАЦИИ ПО чл. 36 И ОТ РЕГЛАМЕНТ (ЕС) 2016/679 И чл. 65 ОТ ЗЗЛД– ДИРЕКЦИЯ „ПАИКД“

1. Неприсъствени действия / Планиране / Предварителна подготовка

1.1. входиране на искането за предварителна консултация в деловодството на КЗЛД;

1.2. определяне на служител / екип от служители за разглеждането на искането;

1.3. анализ на подаденото искане (в едномесечен срок, който спира да тече в случаите, когато от АЛД/ОЛД е изискана допълнителна информация и продължава да тече след нейното получаване):

1.3.1. идентификация на АЛД/ОЛД, подал искането – седалище и адрес на управление, предмета на дейност и др.;

1.3.2. проверка дали АЛД/ОЛД е определил ДЛЗД и уведомена ли е КЗЛД за него, съответно предоставени ли са координати за връзка с него;

1.3.3. информация за съответните отговорности на АЛД, съвместните АЛД и ОЛД, които се занимават с обработването, по-конкретно при обработване на данни в рамките на група предприятия (където е приложимо);

1.3.4. целите на планираното обработване и средствата за него;

1.3.5. описание на предприетите или предложените от АЛД/ОЛД технически и организационни мерки за защита на личните данни (предвидените мерки и гаранции за защита на правата и свободите на субектите на данни);

1.3.6. предоставена ли е оценка на въздействието върху защитата на данните по чл. 35 от Регламент (ЕС) 2016/679;

1.3.7. наличие на становище на ДЛЗД при извършването на оценката на въздействие (чл. 35, § 2 от Регламент (ЕС) 2016/679);

1.3.8. наличие на мнение на заинтересовани страни, в т.ч. субекти на данни (чл. 35, § 9 от Регламент (ЕС) 2016/679);

1.3.9. направен ли е анализ на определения от АЛД/ОЛД висок риск;

1.3.10 описание на новите технологии;

1.3.11. направен ли е анализ на риска, във връзка с въвеждане на новите технологии, механизми или процедури (информационни системи или приложения), които предстои да бъдат внедрени;

1.3.12. описание на естеството на искането;

1.3.13. категории и брой на субекти на данни;

1.3.14. категории и брой засегнати лични данни.

1.4. при необходимост от допълване на информацията, изискуема по чл. 36, § 3 от Регламент (ЕС) 2016/679, се изисква писмено допълнителна информация от АЛД/ОЛД. Ако същата не бъде предоставена в указания срок, се изпраща повторно писмо;

1.5. в случай, че АЛД/ОЛД не предостави исканата информация, се изготвя докладна записка (излагат се само факти), която се докладва на КЗЛД, с оглед вземане на Решение;

1.6. в случай на недопустимост, в едномесечен срок от подаването на искането, се изготвя становище с мотивирано предложение до КЗЛД. При недопустимо искане, АЛД/ОЛД се уведомява, като му се изпраща заверено копие на Решението на КЗЛД.

2. Проверки по документи – анализ по същество

2.1. проучване и анализ на приложимото към искането законодателство и Насоките на Европейския комитет по защита на данните (в т.ч. Насоки относно оценката на въздействието върху защитата на данни (ОВЗД) и определяне дали съществува вероятност обработването „да породи висок риск" за целите на Регламент (ЕС) 2016/679);

2.2. направен ли е анализ на баланса на легитимния интерес на АЛД/ОЛД и правата и свободите на ФЛ при обработването на данните;

2.3. предоставена ли е документация за техническите и функционални характеристики на информационните системи или приложения, които са предмет на искането и предстои да бъдат внедрени от АЛД;

2.4. проучване и анализ на приложима към искането практика – на КЗЛД, на Съда на Европейския съюз;

2.5. предварително проучване на АЛД, в т.ч. има ли подадени жалби, сигнали, уведомления в КЗЛД и откази от съдействие, издадените АУАН и НП;

2.6. проверка за наличието на жалби, депозирани чрез Информационната система на вътрешния пазар;

2.7. извършване на преценка на предвидените мерки за ограничаване на риска при обработването на лични данни;

2.8. анализ на техническите и функционални характеристики на информационните системи или приложения, които са предмет на искането и предстои да бъдат внедрени от АЛД, в контекста на защитата на личните данни (тук биха могли да се включат, но да не се изчерпват с пълното описание на техническите и функционални характеристики на системата, потока от данни, разработчика на технологията, възможности, сертификати по отношение на сигурността и друга релевантна информация);

2.9. проверка за законосъобразно обработване на лични данни съобразно предмета на искането;

2.10. наличие на одити по отношение спазването на Наредбата за минимални изисквания за мрежова и информационна сигурност и ISO 27701 (ако е относимо към предмета на искането);

2.11. проверка на сигурността и сертифициране на информационните системи, обработващи лични данни (ако е относимо към предмета на искането);

2.12. наличие на сертификати за информационна сигурност и за защита на личните данни (ако е относимо към предмета на искането);

2.13. присъединил ли се е АЛД/ОЛД към одобрен Кодекс за поведение (ако е относимо към предмета на искането);

2.14. справки в интернет страници;

2.15. телефонни разговори;

2.16. електронни съобщения;

2.17. справки в публични бази данни;

2.18. изискване на становище/становища (при необходимост);

2.19. събиране и анализ на доказателства за всеки установен факт – документи на хартиен и/или електронен носител (в т.ч. направения анализ на риска и определяне на нивото на въздействие, правила, процедури, становища, екранни разпечатки и др.);

2.20. при необходимост, с оглед сложността на планираното обработване и/или необходимостта от привличане на външен експерт, в едномесечен срок от получаване на искането,се изготвя доклад до КЗЛД за удължаване на срока и/или привличането на външен експерт. При взимане на решение за удължаване на срока, АЛД се информира за удължаването на срока, както и за причините за забавянето;

2.21. в случаите, визирани в чл. 36, § 5 от Регламент (ЕС) 2016/679, във връзка с чл. 12, ал. 2 от ЗЗЛД, следва да се извърши анализна обществения интерес, в т. ч. когато обработването се извършва във връзка със социалната закрила и общественото здраве.

3. Приключване на проверката

3.1. изготвяне на становище за разглеждане и приемане на заседание на КЗЛД с анализ и предложения:

3.1.1. предложение за приемане на искането за приложимо и разрешение възможността за внедряване на новата технология, механизми, процедури (информационни системи или приложения, които предстои да бъдат внедрени);

3.1.2. предложение КЗЛД да приеме Решение за упражняване на правомощията си по чл. 58 от Регламент (ЕС) 2016/679;

3.1.3. предложение КЗЛД да издаде разрешение/отказ за обработване на данни по чл. 36, § 5 от Регламент (ЕС) 2016/679.

4. Последващи действия на КЗЛД

4.1. произнасяне на КЗЛД с Решение;

4.2. изготвяне на писмо до АЛД/ОЛД, към което е приложено заверено копие на акта, с който се е произнесла КЗЛД.

VIII. ПРОВЕРКИ НА СЕРТИФИЦИРАЩИ ОРГАНИ (СО) – ДИРЕКЦИЯ „ПАИКД“

А. Проверки след подаден сигнал

1. Проверки по документи

1.1. входиране на сигнал в деловодството на КЗЛД;

1.2. определяне на служител / екип от служители за разглеждането на сигнала;

1.3. проверка дали СО фигурира в регистъра на КЗЛД;

1.4. предварително проучване на СО:

1.4.1. налице ли е валидно ISO 17065/2012;

1.4.2. проверка на схемата за акредитиране на КЗЛД (ISO 17065/2012 и допълнителните изисквания, формулирани от КЗЛД);

1.4.3. проверка на схемата за сертифициране, изпратена от СО на КЗЛД;

1.4.4. проверка дали СО продължава да отговаря на критериите за акредитация, съгласно Наредба на КЗЛД по чл. 14, ал. 5 от ЗЗЛД;

1.4.5. проверка на срока на акредитацията;

1.4.6. проверка колко сертификата е издал СО и при какви условия;

1.4.7. проверка относно надзора, който СО осъществява върху сертифицираните АЛД;

1.4.8. проверка за спазване на процедура за недопустимост на конфликт на интереси и безпристрастност;

1.4.9. продължават ли да са налични достатъчно ресурси за осъществяването на дейността по сертификация;

1.4.10. има ли подадени жалби, сигнали, уведомления в КЗЛД и откази от съдействие, издадените АУАН и НП.

1.5. проучване на приложимото към казуса законодателство и Насоките на Европейския комитет по защита на данните;

1.6. проучване на приложима към казуса практика – на КЗЛД, на Съда на Европейския съюз;

1.7. справки в публични бази данни;

1.8. справки в интернет страници;

1.9. телефонни разговори;

1.10. електронни съобщения;

1.11. изискване на становище/становища;

1.12. искане на становище/становища (при необходимост);

1.13. анализ на събраните в хода на проверката документи, в т.ч. Насоките на Европейския комитет по защита на данните и решенията на Съда на Европейския съюз, приложими към казуса;

1.15. анализ на сключените договори с физически или юридически лица и наличието на клаузи, регламентиращи обработването на личните данни;

1.16. изготвяне на отговор до сигналоподателя, без да се предприемат последващи действия;

1.17. сигналът да се препрати по компетентност на друг орган/органи;

1.18. в зависимост от казуса на сигнала и събраните документи следва:

1.18.1. да се изготви констативен акт, който да се докладва на КЗЛД със съответните предложения на служителя, разглеждащ сигнала. Констативният акт може да съдържа предложения за приемане при липса на нарушение, за преквалифицирането на сигнала в жалба, за отнемане на акредитацията, за извършване на проверка на място (с предложение за членовете на екипите за проверки и привличане на външен експерт при необходимост), за издаване на корективна мярка по чл. 58, § 2 от Регламент (ЕС) 2016/679, за препращане на събраната документация на друг компетентен орган, включително по Информационната система на вътрешния пазар и др.;

1.18.2 да се състави АУАН/НП само на база на събрани документи, без проверка на място, като задължително служителите на дирекция „ПАИКД“ следва да предприемат действия за потвърждение на фактите и обстоятелствата, съдържащи се в документите и събирането на допълнителни писмени материали, с оглед упражняването на правомощията на КЗЛД;

1.19. при получаване на документи, изпратени по компетентност на КЗЛД от Прокуратурата на Република България / МВР и други органи се изготвя докладна записка до КЗЛД с предложения:

1.19.1 препращане по компетентност на друг орган / органи;

1.19.2 издаване на корективна мяркапо чл. 58, § 2 от Регламент (ЕС) 2016/679;

1.19.3 стартиране на процедура по ЗАНН със съставяне на АУАН по документи, като служителите на дирекция „ПАИКД“ следва задължително да предприемат действия за потвърждение на фактите и обстоятелствата, съдържащи се в

документите и събирането на допълнителни писмени материали, с оглед упражняването на правомощията на КЗЛД.

1.20. изготвяне на отговор до сигналоподателя, съдържащ информация за предприетите от КЗЛД действия, с препращане към друг орган / издаване на корективна мярка / налагане на санкция.

2. Проверки на място на СО – дирекция „ПАИКД“

2.1. Неприсъствени действия / Планиране / Предварителна подготовка:

2.1.1. приемане на Решение на КЗЛД за извършване на проверка на място;

2.1.2. издаване на заповед за проверка с определяне на екипа за проверка, предмета, обхвата и целите на проверката, включително привличане на външен експерт (при необходимост) – два оригинала;

2.1.3. изпращане на уведомително писмо с въпросник (при необходимост), включително и по електронен път.

2.2. Проверка на място в седалището/обект на СО:

2.2.1. легитимиране на проверяващия екип със служебни карти;

2.2.2. легитимация на представляващия СО;

2.2.3. връчване на заповедта на председателя на КЗЛД за извършване на проверката – връчва се оригинал на заповедта, като на екземпляра на проверяващия екип представляващия СО или упълномощеното от него лице собственоръчно написва текст, че е получил копие от заповедта за проверка, датата, трите си имена и подпис (за юридическите лица – печат, при възможност);

2.2.4. изясняване на факти и обстоятелства по отношение на получения сигнал;

2.2.5. проверка за законосъобразно обработване на лични данни съобразно предмета на сигнала и задачата на проверката (ако е относимо към проверката);

2.2.6. изясняване на факти и обстоятелства по отношение на дейността на СО – събиране на документация и доказателства, кореспондиращи с предварителното проучване на СО;

2.2.7. наличие на одити по отношение спазването на Наредбата за минимални изисквания за мрежова и информационна сигурност и ISO 27701 (ако е относимо към предмета на сигнала);

2.2.8. проверка на сигурността и сертифициране на информационните системи, обработващи лични данни (ако е относимо към предмета на сигнала);

2.2.9. наличие на сертификати за информационна сигурност и за защита на личните данни (ако е относимо към предмета на сигнала);

2.2.10. присъединил ли се е СО към одобрен кодекс за поведение (ако е относимо към предмета на сигнала);

2.2.11. събиране на доказателства за всеки установен факт – документи на хартиен и/или електронен носител (в т.ч. направения анализ на риска и определяне на нивото на въздействие, правила, процедури, становища, екранни разпечатки и др.), като задължително СО предоставя заверени копия на сключени договори с физически или юридически лица, касаещи обработването на лични данни;

2.2.12. изготвяне на констативен протокол по време на проверката, екземпляр се връчва на СО;

2.2.13. изготвяне на приемо-предавателен протокол със заверени копия на документи и предоставени доказателства от СО, екземпляр се връчва на СО;

2.2.14. указване на срок за предоставяне на допълнителни документи (при необходимост).

3. Приключване на проверката

3.1. изготвяне на констативен акт и завеждането му в деловодната система, ведно с приложените в оригинал документи и доказателства, като задължително включва мнение и предложения на проверяващия екип:

3.1.1. предложение за приемане при липса на нарушение;

3.1.2. за отнемане на акредитацията;

3.1.3. предложение за издаване на корективна мярка по чл. 58, § 2 от Регламент (ЕС) 2016/679;

3.1.4. при установяване на административно нарушение – предложение за налагане на санкция на СО, със стартиране на производство по ЗАНН със съставяне и връчване на АУАН.

3.2. констативният акт се внася за разглеждане и приемане на заседание на КЗЛД.

4. Последващи действия на КЗЛД

4.1. приемане с Решение на изготвения констативен акт;

4.2. изготвяне на писмо до АЛД с констатации от проверката (когато няма наложена корективна мярка);

4.3. при отнемане на акредитацията – на СО се изпраща заверено копие на Решението на КЗЛД;

4.4. при издаване на корективна мярка по чл. 58, § 2 от Регламент (ЕС) 2016/679:

4.4.1. Решение на КЗЛД − диспозитивът на Решението задължително съдържа издадената корективна мярка (разпореждане), срок за нейното изпълнение, срок за представяне на доказателства за изпълнението му от СО, информация за административно-наказателната отговорност, която носи СО в случай, че не го изпълни или не изпрати доказателства за изпълнението му в указания срок, както и за възможността за обжалване пред съответния съд;

4.4.2. Решението се връчва на съответния СО;

4.4.3. след изтичане на 14-дневен срок влиза в сила и подлежи на изпълнение, ако ответната страна не оспорва Решението;

4.4.4. предоставяне на писмени доказателства от СО за изпълнение на коректвината мярка и докладване на заседание на КЗЛД;

4.4.5. ако в указания срок СО не представи доказателства за изпълнение на коректвината мярка:

а) изпраща се напомнително писмо с обратна разписка с указан 7-дневен срок, в който СО следва да предостави доказателства и/или становище за изпълнение на решението на КЗЛД и нейните разпореждания, както и информация за административно-наказателната отговорност, която носи СО в случай, че не го изпълни;

б) при изпълнение на указаното с писмото се изготвя докладна записка до КЗЛД с предложение за приемане;

в) в случай на неизпълнение на указаното с писмото се изготвя докладна записка до КЗЛД с предложение за налагане на административна санкцияпо реда на чл. 83, § 6 от Регламент (ЕС) 2016/679 и чл. 84 от ЗЗЛД, която се докладва на КЗЛД;

г) вземане на Решение на КЗЛД.

4.5. издадените констативни актове се присъединяват към преписката;

4.6. издадените АУАН, НП и решенията за корективни мерки по чл. 58, § 2 от Регламент (ЕС) 2016/679 се вписват и съхраняват в съответния регистър.

Б. Проверки на СО при висок обществен интерес / Самосезиране на КЗЛД

1. Проверки по документи

1.1. приемане на Решение на КЗЛД за самосезиране, в т.ч. при възникване на казус с висок обществен интерес;

1.2. определяне на служител / екип от служители за извършване на проверка по документи;

1.3. предварително проучване на СО:

1.3.1. проверка дали СО фигурира в регистъра на КЗЛД;

1.3.2. налице ли е валидно ISO 17065/2012;

1.3.3. проверка на схемата за акредитиране на КЗЛД (ISO 17065/2012 и допълнителните изисквания, формулирани от КЗЛД);

1.3.4. проверка на схемата за сертифициране, изпратена от СО на КЗЛД;

1.3.5. проверка дали СО продължава да отговаря на критериите за акредитация, съгласно Наредба на КЗЛД по чл. 14, ал. 5 от ЗЗЛД;

1.3.6. проверка на срока на акредитацията;

1.3.7. проверка колко сертификата е издал СО и при какви условия;

1.3.8. проверка относно надзора, който СО осъществява върху сертифицираните АЛД;

1.3.9. проверка за спазване на процедура за недопустимост на конфликт на интереси и безпристрастност;

1.3.10. продължават ли да са налични достатъчно ресурси за осъществяването на дейността по сертификация;

1.3.11. има ли подадени жалби, сигнали, уведомления в КЗЛД и откази от съдействие, издадените АУАН и НП.

1.4. събиране на документи за изясняване на факти и обстоятелства по предмета на самосезирането:

1.4.1. проучване на приложимото към казуса законодателство и Насоките на Европейския комитет по защита на данните;

1.4.2. проучване на приложима към казуса практика – на КЗЛД, на Съда на Европейския съюз;

1.4.3. справки в публични бази данни;

1.4.4. справки в интернет страници;

1.4.5. телефонни разговори;

1.4.6. електронни съобщения;

1.4.7. изискване на становище/становища;

1.4.8. искане на становище/становища (при необходимост);

1.4.9. изпращане на уведомително писмо за проверката до всички СО с приложен въпросник, включително и по електронен път.

1.5. анализ на събраните в хода на проверката документи, в т.ч. Насоките на Европейския комитет по защита на данните и решенията на Съда на Европейския съюз, приложими към казуса;

1.6. анализ на сключените договори с физически или юридически лица и наличието на клаузи, регламентиращи обработването на личните данни;

1.7. в зависимост от казуса и събраните документи следва:

1.7.1 да се изготви констативен акт, който да се докладва на КЗЛД със съответните предложения на служителя/ите. Констативният акт може да съдържа предложения за приемане при липса на нарушение, за отнемане на акредитацията, за извършване на проверка на място (с предложение за членовете на екипите за проверки и привличане на външен експерт при необходимост), за издаване на корективна мярка по чл. 58, § 2 от Регламент (ЕС) 2016/679, за препращане на събраната документация на друг компетентен орган, включително по Информационната система на вътрешния пазар и др.;

1.7.2. да се състави АУАН/НП само на база на събрани документи, без проверка на място, като задължително служителите на дирекция „ПАИКД“ следва да предприемат действия за потвърждение на фактите и обстоятелствата, съдържащи се в документите и събирането на допълнителни писмени материали, с оглед упражняването на правомощията на КЗЛД.

2. Проверки на място на СО – дирекция „ПАИКД“

2.1. Неприсъствени действия / Планиране / Предварителна подготовка:

2.1.1. приемане на решение на КЗЛД за извършване на проверка на място с определяне на предмета, обхвата и целите на проверката, включително привличане на външен експерт (при необходимост);

2.1.2. издаване на заповед за проверка с определяне на екипа за проверка – два оригинала;

2.1.3. изпращане на уведомително писмо за проверката до СО с приложен въпросник, включително и по електронен път.

2.2. Проверка на място в седалището/обект на СО

2.2.1. легитимиране на проверяващия екип със служебни карти;

2.2.2. легитимация на представляващия СО;

2.2.3. връчване на заповедта на председателя на КЗЛД за извършване на проверката – връчва се оригинал на заповедта, като на екземпляра на проверяващия екип представляващия СО или упълномощеното от него лице собственоръчно написва текст, че е получил копие от заповедта за проверка, датата, трите си имена и подпис (за юридическите лица – печат, при възможност);

2.2.4. проверка за законосъобразно обработване на лични данни съобразно предмета и задачата на проверката (ако е относимо към проверката);

2.2.5. задължителна проверка и събиране на доказателства относно:

а) дейността на СО – събиране на документация и доказателства, кореспондиращи с предварителното проучване на СО;

б) наличие на одити по отношение спазването на Наредбата за минимални изисквания за мрежова и информационна сигурност и ISO 27701;

в)проверка на сигурността и сертифициране на информационните системи, обработващи лични данни;

г) наличие на сертификати за информационна сигурност и за защита на личните данни;

2.2.6. в случай, че е относимо към проверката, събиране на доказателства относно:

а) спазване принципите за законосъобразно обработване на лични данни (чл. 5, 6 от Регламент (ЕС) 2016/679);

б) условията за даване на съгласие (чл. 7 от Регламент (ЕС) 2016/679);

в) условията, приложими за съгласието на дете във връзка с услугите на информационното общество (чл. 8 от Регламент (ЕС) 2016/679);

г) обработването на специални категории лични данни (чл. 9 от Регламент (ЕС) 2016/679);

д) предприетите от СО действия за информиране на физическите лица за целите на обработване на личните им данни и упражняването на техните права съгласно чл. 15–22 от Регламент (ЕС) 2016/679;

е) предаване на лични данни на трети държави или международни организации (чл. 44–50 от Регламент (ЕС) 2016/679) – на кои, основанието и начин на предаване, категории лични данни, технически и организационни мерки за защита;

ж) обмен на лични данни с български институции – на кои, основанието и начин на предаване, категории лични данни, технически и организационни мерки за защита;

з) предприетите технически и организационни мерки за защита на личните данни;

и) присъединил ли се е СО към одобрен кодекс за поведение (ако е относимо);

й) събиране на доказателства за всеки установен факт – документи на хартиен и/или електронен носител (в т.ч. направения анализ на риска и определяне на нивото на въздействие, правила, процедури, становища, екранни разпечатки и др.), като

задължително СО предоставя заверени копия на сключени договори с физически или юридически лица, касаещи обработването на лични данни.

2.2.7. изготвяне на констативен протокол по време на проверката, екземпляр се връчва на СО;

2.2.8. изготвяне на приемо-предавателен протокол със заверени копия на документи и предоставени доказателства от СО, екземпляр се връчва на СО;

2.2.9. указване на срок за предоставяне на допълнителни документи (при необходимост).

3. Приключване на проверката

3.1. изготвяне на констативен акт и завеждането му в деловодната система, ведно с приложените в оригинал документи и доказателства, като задължително включва мнение и предложения на проверяващия екип:

3.1.1. предложение за приемане при липса на нарушение;

3.1.2. за отнемане на акредитацията;

3.1.3. предложение за издаване на корективна мярка по чл. 58, § 2 от Регламент (ЕС) 2016/679;

3.1.4. при установяване на административно нарушение – предложение за налагане на санкция на СО, със стартиране на производство по ЗАНН със съставяне и връчване на АУАН.

3.2. констативният акт се внася за разглеждане и приемане на заседание на КЗЛД.

4. Последващи действия на КЗЛД

4.1. приемане с Решение на изготвения констативен акт;

4.2. изготвяне на писмо до СО с констатации от проверката (когато няма наложена корективна мярка);

4.3. при отнемане на акредитацията – на СО се изпраща заверено копие на Решението на КЗЛД;

4.4. при издаване на корективна мярка по чл. 58, § 2 от Регламент (ЕС) 2016/679:

4.4.1. Решение на КЗЛД – диспозитивът на Решението задължително съдържа издадената корективна мярка (разпореждане), срок за нейното изпълнение, срок за представяне на доказателства за изпълнението му от СО, информация за административно-наказателната отговорност, която носи СО в случай, че не го изпълни

или не изпрати доказателства за изпълнението му в указания срок, както и за възможността за обжалване пред съответния съд;

4.4.2. Решението се връчва на съответния СО;

4.4.3. след изтичане на 14-дневен срок влиза в сила и подлежи на изпълнение, ако ответната страна не оспорва Решението;

4.4.4. предоставяне на писмени доказателства от СО за изпълнение на корективната мярка и докладване на заседание на КЗЛД;

4.4.5. ако в указания срок СО не представи доказателства за изпълнение на корективната мярка:

а) изпраща се напомнително писмо с обратна разписка с указан 7-дневен срок, в който СО следва да предостави доказателства и/или становище за изпълнение на решението на КЗЛД и нейните разпореждания, както и информация за административно-наказателната отговорност, която носи СО в случай, че не го изпълни;

б) при изпълнение на указаното с писмото, се изготвя докладна записка до КЗЛД с предложение за приемане;

в) в случай на неизпълнение на указаното с писмото, се изготвя докладна записка до КЗЛД с предложение за налагане на административна санкция по реда на чл. 83, § 6 от Регламент (ЕС) 2016/679 и чл. 84 от ЗЗЛД, която се докладва на КЗЛД;

г) вземане на Решение на КЗЛД.

4.5. издадените констативни актове се присъединяват към преписката;

4.6. издадените АУАН, НП и решенията за корективни мерки по чл. 58, § 2 от Регламент (ЕС) 2016/679 се вписват и съхраняват в съответния регистър.

В. Секторни/планови проверки на СО

1. Неприсъствени действия / Планиране / Предварителна подготовка

1.1. изготвяне на докладна записка с предложение за вземане на Решение на КЗЛД за извършване на планова проверка на СО на база на следните критерии:

1.1.1. обществена значимост на нарушенията, сигнализирани с жалби и сигнали;

1.1.2. повтаряемост на нарушенията;

1.1.3. промяна на законодателството;

1.1.4. други…….

1.2. докладната записка се внася за разглеждане и приемане на заседание на КЗЛД;

1.3. приемане на Решение на КЗЛД за извършване на планова проверка с определяне на предмета, обхвата, субектите и целите на проверката, вкл. привличане на външен експерт (при необходимост).

2. Проверки по документи

2.1. анализ на СО, на които ще бъде извършена проверка, по горепосочените критерии / предварително проучване на СО:

2.1.1. проверка дали СО фигурират в регистъра на КЗЛД;

2.1.2. налице ли е валидно ISO 17065/2012;

2.1.3. проверка на схемата за акредитиране на КЗЛД (ISO 17065/2012 и допълнителните изисквания, формулирани от КЗЛД);

2.1.4. проверка на схемата за сертифициране, изпратени от СО на КЗЛД;

2.1.5. проверка дали СО продължават да отговаря на критериите за акредитация, съгласно Наредба на КЗЛД по чл. 14, ал. 5 от ЗЗЛД;

2.1.6. проверка на срока на акредитацията;

2.1.7. проверка колко сертификата са издали СО и при какви условия;

2.1.8. проверка относно надзора, който СО осъществяват върху сертифицираните от тях АЛД;

2.1.9. проверка за спазване на процедура за недопустимост на конфликт на интереси и безпристрастност;

2.1.10. продължават ли да са налични достатъчно ресурси за осъществяването на дейността по сертификация;

2.1.11. има ли подадени жалби, сигнали, уведомления в КЗЛД и откази от съдействие, издадените АУАН и НП за всеки от СО, обект на проверката.

2.2. проучване на приложимото към казуса законодателство и Насоките на Европейския комитет по защита на данните;

2.3. проучване на приложима към казуса практика – на КЗЛД, на Съда на Европейския съюз;

2.4. справки в публични бази данни;

2.5. справки в интернет страници;

2.6. телефонни разговори;

2.7. електронни съобщения;

2.8. изискване на становище/становища;

2.9. искане на становище/становища (при необходимост);

2.10. изпращане на уведомително писмо за проверката до всички СО с приложен въпросник, включително и по електронен път;

2.11. анализ на събраните в хода на проверката документи, в т.ч. Насоките на Европейския комитет по защита на данните и решенията на Съда на Европейския съюз, приложими към казуса;

2.12. анализ на сключените договори с физически или юридически лица и наличието на клаузи, регламентиращи обработването на личните данни;

2.13. изготвяне на констативен акт за всеки СО със предложение за приемане при липса на нарушение, за отнемане на акредитацията, за извършване на проверка на място (с предложение за членовете на екипите за проверки и привличане на външен експерт при необходимост), за издаване на корективна мярка по чл. 58, § 2 от Регламент (ЕС) 2016/679, за препращане на събраната документация на друг компетентен орган, включително по Информационната система на вътрешния пазар и др.;

2.14 констативните актове се внасят за разглеждане и приемане на заседание на КЗЛД;

2.15. при констатирано нарушение се изготвя АУАН/НП само на база на събрани документи, без проверка на място, като задължително служителите на дирекция „ПАИКД“ следва да предприемат действия за потвърждение на фактите и обстоятелствата, съдържащи се в документите и събирането на допълнителни писмени материали, с оглед упражняването на правомощията на КЗЛД.

3. Проверки на място на СО – дирекция „ПАИКД“

3.1. Неприсъствени действия / Планиране / Предварителна подготовка:

3.1.1. приемане на Решение на КЗЛД за извършване на проверка на мястос определяне на предмета, обхвата, субектите и целите на проверката, вкл. привличане на външен експерт (при необходимост);

3.1.2. издаване на заповед за проверка с определяне на екипа за проверка – два оригинала;

3.1.3. разписване на функции и отговорности на членовете на екипите за проверки;

3.1.4. изготвяне на хронограма за действията на екипа (при необходимост);

3.1.5. изпращане на уведомително писмо за проверката до всички СО с приложен въпросник, включително и по електронен път.

3.2. Проверка на място в седалището/обект на СО:

3.2.1. легитимиране на проверяващия екип със служебни карти на място;

3.2.3. легитимация на представляващия СО;

3.2.3. връчване на заповедта на председателя на КЗЛД за извършване на проверката – връчва се оригинал на заповедта, като на екземпляра на проверяващия екип представляващия СО или упълномощеното от него лице собственоръчно написва текст, че е получил копие от заповедта за проверка, датата, трите си имена и подпис (за юридическите лица – печат, при възможност);

3.2.4. проверка за законосъобразно обработване на лични данни съобразно предмета и задачата на проверката (ако е относимо към проверката);

3.2.5. задължителна проверка и събиране на доказателства относно:

а) дейността на СО – събиране на документация и доказателства, кореспондиращи с предварителното проучване на СО;

б) наличие на одити по отношение спазването на Наредбата за минимални изисквания за мрежова и информационна сигурност и ISO 27701;

в) проверка на сигурността и сертифициране на информационните системи, обработващи лични данни;

г) наличие на сертификати за информационна сигурност и за защита на личните данни.

3.2.6. в случай, че е относимо към проверката, събиране на доказателства относно:

а) спазване принципите за законосъобразно обработване на лични данни (чл. 5, 6 от Регламент (ЕС) 2016/679);

б) условията за даване на съгласие (чл. 7 от Регламент (ЕС) 2016/679);

в) условията, приложими за съгласието на дете във връзка с услугите на информационното общество (чл. 8 от Регламент (ЕС) 2016/679);

г) обработването на специални категории лични данни (чл. 9 от Регламент (ЕС) 2016/679);

д) предприетите от СО действия за информиране на физическите лица за целите на обработване на личните им данни и упражняването на техните права съгласно чл. 15–22 от Регламент (ЕС) 2016/679;

е) предаване на лични данни на трети държави или международни организации (чл. 44–50 от Регламент (ЕС) 2016/679) − на кои, основанието и начин на предаване, категории лични данни, технически и организационни мерки за защита;

ж) обмен на лични данни с български институции – на кои, основанието и начин на предаване, категории лични данни, технически и организационни мерки за защита;

з) предприетите технически и организационни мерки за защита на личните данни;

и) присъединил ли се е СО към одобрен кодекс за поведение (ако е относимо);

й) събиране на доказателства за всеки установен факт – документи на хартиен и/или електронен носител (в т.ч. направения анализ на риска и определяне на нивото на въздействие, правила, процедури, становища, екранни разпечатки и др.), като задължително СО предоставя заверени копия на сключени договори с физически или юридически лица, касаещи обработването на лични данни.

3.2.7. изготвяне на констативен протокол по време на проверката, екземпляр се връчва на СО;

3.2.8. изготвяне на приемо-предавателен протокол със заверени копия на документи и предоставени доказателства от СО, екземпляр се връчва на СО;

3.2.9. указване на срок за предоставяне на допълнителни документи (при необходимост).

3.3. Приключване на проверката на място:

3.3.1. изготвяне на констативен акт и завеждането му в деловодната система, ведно с приложените в оригинал документи и доказателства, като задължително включва мнение и предложения на проверяващия екип:

а) предложение за приемане при липса на нарушение;

б) за отнемане на акредитацията;

в) предложение за издаване на корективна мярка по чл. 58, § 2 от Регламент (ЕС) 2016/679;

г) при установяване на административно нарушение – предложение за налагане на санкция на СО, със стартиране на производство по ЗАНН със съставяне и връчване на АУАН.

3.3.2. приемане с Решение на КЗЛД на изготвените констативни актове.

4. Приключване на Секторната проверка / Плановата проверка / Одита

4.1. изготвяне на окончателен доклад за Секторната проверка / Плановата проверка / Одита, съдържащ обобщен анализ на извършените проверки (по документи и на място), заключения и предложения до КЗЛД за изготвяне на препоръки към всички СО (при необходимост);

4.2. внасяне на окончателния доклад за разглеждане и приемане на заседание на КЗЛД.

5. Последващи действия на КЗЛД

5.1. запознаване и приемане от КЗЛД на окончателен доклад за Секторната проверка / Плановата проверка / Одита и одобрение на препоръки към всички СО (при необходимост);

5.2. публикуване на анонимизиран окончателен доклад и препоръките на интернет страницата на КЗЛД;

5.3. изготвяне на писмо до съответните СО с констатации от проверката (когато няма наложена корективна мярка);

5.4. при отнемане на акредитацията – на съответните СО се изпраща заверено копие на Решението на КЗЛД;

5.5. при издаване на корективна мярка по чл. 58, § 2 от Регламент (ЕС) 2016/679:

5.5.1. Решение на КЗЛД − диспозитивът на Решението задължително съдържа издадената корективна мярка (разпореждане), срок за нейното изпълнение, срок за представяне на доказателства за изпълнението му от СО, информация за административно-наказателната отговорност, която носи СО в случай, че не го изпълни или не изпрати доказателства за изпълнението му в указания срок, както и за възможността за обжалване пред съответния съд;

5.5.2. Решението се връчва на съответния СО;

5.5.3. след изтичане на 14-дневен срок влиза в сила и подлежи на изпълнение, ако ответната страна не оспорва Решението;

5.5.4. предоставяне на писмени доказателства от СО за изпълнение на корективната мярка и докладване на заседание на КЗЛД;

5.5.5. ако в указания срок СО не представи доказателства за изпълнение на корективната мярка:

а) изпраща се напомнително писмо с обратна разписка с указан 7-дневен срок, в който СО следва да предостави доказателства и/или становище за изпълнение на решението на КЗЛД и нейните разпореждания, както и информация за административно-наказателната отговорност, която носи СО в случай, че не го изпълни;

б) при изпълнение на указаното с писмото, се изготвя докладна записка до КЗЛД с предложение за приемане;

в) в случай на неизпълнение на указаното с писмото, се изготвя докладна записка до КЗЛД с предложение за налагане на административна санкция по реда на чл. 83, § 6 от Регламент (ЕС) 2016/679 и чл. 84 от ЗЗЛД, която се докладва на КЗЛД;

г) вземане на Решение на КЗЛД.

5.6. издадените констативни актове се присъединяват към преписката;

5.7. издадените АУАН, НП и решенията за корективни мерки по чл. 58, § 2 от Регламент (ЕС) 2016/679 се вписват и съхраняват в съответния регистър.

IX. ПРОВЕРКИ НА СЕРТИФИЦИРАНИ АЛД – ДИРЕКЦИЯ „ПАИКД“

А. Проверки след подаден сигнал

1. Проверки по документи

1.1. входиране на сигнал в деловодството на КЗЛД;

1.2. определяне на служител / екип от служители за разглеждането на сигнала;

1.3. предварително проучване на сертифицирания АЛД:

1.3.1. кой е СО, издал сертификата;

1.3.2. проверка дали сертифицирания АЛД отговаря на критериите, визирани в Наредба на КЗЛД по чл. 14, ал. 6 от ЗЗЛД;

1.3.3. проверка относно обхвата/предмета на сертифициране;

1.3.4. оценка на схемата за сертификация;

1.3.5. проверка на разпределение на нива и отговорности;

1.3.6. проверка на цялата релевантна документация;

1.3.7. на какъв период се извършва проверка от страна на СО, както и документацията, обективираща резултатите от тази проверка;

1.3.8. проверка за това дали се съблюдават стандартите ISO тогава, когато това е приложимо;

1.3.9. за какъв период е сертификацията и дали е валидна към момента;

1.3.10. има ли подадени жалби, сигнали, уведомления в КЗЛД и откази от съдействие, издадените АУАН и НП.

1.4. проучване на приложимото към казуса законодателство и Насоките на Европейския комитет по защита на данните;

1.5. проучване на приложима към казуса практика – на КЗЛД, на Съда на Европейския съюз;

1.6. справки в публични бази данни;

1.7. справки в интернет страници;

1.8. телефонни разговори;

1.9. електронни съобщения;

1.10. изискване на становище/становища;

1.11. искане на становище/становища (при необходимост);

1.12. анализ на събраните в хода на проверката документи, в т.ч. Насоките на Европейския комитет по защита на данните и решенията на Съда на Европейския съюз, приложими към казуса;

1.13. анализ на сключените договори с физически или юридически лица и наличието на клаузи, регламентиращи обработването на личните данни;

1.14. изготвяне на отговор до сигналоподателя, без да се предприемат последващи действия;

1.15. сигналът да се препрати по компетентност на друг орган/органи;

1.16. в зависимост от казуса на сигнала и събраните документи следва:

1.16.1. да се изготви констативен акт, който да се докладва на КЗЛД със съответните предложения на служителя, разглеждащ сигнала. Констативният акт може да съдържа предложения за приемане при липса на нарушение, за преквалифицирането на сигнала в жалба, за извършване на проверка на място (с предложение за членовете на екипите за проверки и привличане на външен експерт при необходимост), за издаване на корективна мярка по чл. 58, § 2 от Регламент (ЕС) 2016/679, за препращане на сигнала на друг компетентен орган, включително по Информационната система на вътрешния пазар и др.;

1.16.2. да се състави АУАН/НП само на база на събрани документи, без проверка на място, като задължително служителите на дирекция „ПАИКД“ следва да предприемат действия за потвърждение на фактите и обстоятелствата, съдържащи се в документите и събирането на допълнителни писмени материали, с оглед упражняването на правомощията на КЗЛД;

1.17. при получаване на документи, изпратени по компетентност на КЗЛД от Прокуратурата на Република България / МВР и други органи:

1.17.1 препращане по компетентност на друг орган / органи;

1.17.2 издаване на корективна мяркапо чл. 58, § 2 от Регламент (ЕС) 2016/679;

1.17.3 стартиране на процедура по ЗАНН със съставяне на АУАН по документи, като служителите на дирекция „ПАИКД“ следва задължително да предприемат действия за потвърждение на фактите и обстоятелствата, съдържащи се в документите и събирането на допълнителни писмени материали, с оглед упражняването на правомощията на КЗЛД.

1.18. изготвяне на отговор до сигналоподателя, съдържащ информация за предприетите от КЗЛД действия, с препращане към друг орган / издаване на корективна мярка / налагане на санкция.

2. Проверки на място на сертифицирани АЛД – дирекция „ПАИКД“

2.1. Неприсъствени действия / Планиране / Предварителна подготовка:

2.1.1. приемане на Решение на КЗЛД за извършване на проверка на място;

2.1.2. издаване на заповед за проверка с определяне на екипа за проверка, предмета, обхвата и целите на проверката, включително привличане на външен експерт (при необходимост) – два оригинала;

2.1.3. изпращане на уведомително писмо с въпросник (при необходимост), включително и по електронен път.

2.2. Проверка на място в седалището/обект на сертифицирани АЛД:

2.2.1. легитимиране на проверяващия екип със служебни карти;

2.2.2. легитимация на сертифицирания АЛД;

2.2.3. връчване на заповедта на председателя на КЗЛД за извършване на проверката – връчва се оригинал на заповедта, като на екземпляра на проверяващия екип сертифицирания АЛД или упълномощеното от него лице собственоръчно написва текст, че е получил копие от заповедта за проверка, датата, трите си имена и подпис (за юридическите лица – печат, при възможност);

2.2.4 изясняване на факти и обстоятелства по отношение на получения сигнал;

2.2.5. изясняване на факти и обстоятелства по отношение на дейността на сертифицирания АЛД – събиране на документация и доказателства, кореспондиращи с предварителното проучване на сертифицирания АЛД;

2.2.6. проверка за законосъобразно обработване на лични данни съобразно предмета на сигнала и задачата на проверката;

2.2.7. наличие на одити по отношение спазването на Наредбата за минимални изисквания за мрежова и информационна сигурност и ISO 27701 (ако е относимо към предмета на сигнала);

2.2.8. проверка на сигурността и сертифициране на информационните системи, обработващи лични данни (ако е относимо към предмета на сигнала);

2.2.9. наличие на сертификати за информационна сигурност и за защита на личните данни (ако е относимо към предмета на сигнала);

2.2.10. присъединил ли се е сертифицирания АЛД към одобрен кодекс за поведение (ако е относимо към предмета на сигнала);

2.2.11. събиране на доказателства за всеки установен факт – документи на хартиен и/или електронен носител (в т.ч. направения анализ на риска и определяне на нивото на въздействие, правила, процедури, становища, екранни разпечатки и др.), като

задължително сертифицираният АЛД предоставя заверени копия на сключени договори с физически или юридически лица, касаещи обработването на лични данни;

2.2.12. изготвяне на констативен протокол по време на проверката, екземпляр се връчва на сертифицирания АЛД;

2.2.13. изготвяне на приемо-предавателен протокол със заверени копия на документи и предоставени доказателства от сертифицирания АЛД, екземпляр се връчва на сертифицирания АЛД;

2.2.14. указване на срок за предоставяне на допълнителни документи (при необходимост).

3. Приключване на проверката

3.1. изготвяне на констативен акт и завеждането му в деловодната система, ведно с приложените в оригинал документи и доказателства, като задължително включва мнение и предложения на проверяващия екип:

3.1.1. предложение за приемане при липса на нарушение;

3.1.2. предложение за издаване на корективна мярка по чл. 58, § 2 от Регламент (ЕС) 2016/679;

3.1.3. при установяване на административно нарушение – предложение за налагане на санкция на сертифицирания АЛД, със стартиране на производство по ЗАНН със съставяне и връчване на АУАН.

3.2. констативният акт се внася за разглеждане и приемане на заседание на КЗЛД.

4. Последващи действия на КЗЛД

4.1. приемане с Решение на изготвения констативен акт;

4.2. изготвяне на писмо до сертифицирания АЛД с констатации от проверката (когато няма наложена корективна мярка);

4.3. при издаване на корективна мярка по чл. 58, § 2 от Регламент (ЕС) 2016/679:

4.3.1. Решение на КЗЛД − диспозитивът на Решението задължително съдържа издадената корективна мярка (разпореждане), срок за нейното изпълнение, срок за представяне на доказателства за изпълнението му от сертифицирания АЛД, информация за административно-наказателната отговорност, която носи сертифицираният АЛД в случай, че не го изпълни или не изпрати доказателства за изпълнението му в указания срок, както и за възможността за обжалване пред съответния съд;

4.3.2. Решението се връчва на сертифицирания АЛД;

4.3.3. след изтичане на 14-дневен срок влиза в сила и подлежи на изпълнение, ако ответната страна не оспорва Решението;

4.3.4. предоставяне на писмени доказателства от сертифицирания АЛД за изпълнение на корективната мярка и докладване на заседание на КЗЛД;

4.3.5. ако в указания срок сертифицирания АЛД не представи доказателства за изпълнение на корективната мярка:

а) изпраща се напомнително писмо с обратна разписка с указан 7-дневен срок, в който сертифицирания АЛД следва да предостави доказателства и/или становище за изпълнение на решението на КЗЛД и нейните разпореждания, както и информация за административно-наказателната отговорност, която носи сертифицираният АЛД в случай, че не го изпълни;

б) при изпълнение на указаното с писмото, се изготвя докладна записка до КЗЛД с предложение за приемане;

в) в случай на неизпълнение на указаното с писмото, се изготвя докладна записка до КЗЛД с предложение за налагане на административна санкцияпо реда на чл. 83, § 6 от Регламент (ЕС) 2016/679 и чл. 84 от ЗЗЛД, която се докладва на КЗЛД;

г) вземане на Решение на КЗЛД.

4.3.6. при прилагане на корективна мярка по чл. 58, § 2, буква „з“ от Регламент (ЕС) 2016/679*(„...да разпореди на сертифициращия орган да отнеме сертификат.....“)*, се уведомява съответния СО.

4.4. издадените констативни актове се присъединяват към преписката;

4.5. издадените АУАН, НП и решенията за корективни мерки по чл. 58, § 2 от Регламент (ЕС) 2016/679 се вписват и съхраняват в съответния регистър.

Б. Проверки на сертифицирани АЛД при висок обществен интерес / Самосезиране на КЗЛД

1. Проверки по документи

1.1. приемане на Решение на КЗЛД за самосезиране, в т.ч. при възникване на казус с висок обществен интерес;

1.2. определяне на служител / екип от служители за извършване на проверка по документи;

1.3. предварително проучване на сертифицирания АЛД:

1.3.1. кой е СО, издал сертификата;

1.3.2. проверка дали сертифицирания АЛД отговаря на критериите, визирани в Наредба на КЗЛД по чл. 14, ал. 6 от ЗЗЛД;

1.3.4. проверка относно обхвата/предмета на сертифициране;

1.3.5. оценка на схемата за сертификация;

1.3.6. проверка на разпределение на нива и отговорности;

1.3.7. проверка на цялата релевантна документация;

1.3.8. на какъв период се извършва проверка от страна на СО, както и документацията, обективираща резултатите от тази проверка;

1.3.9. проверка за това дали се съблюдават стандартите ISO тогава, когато това е приложимо;

1.3.10. за какъв период е сертификацията и дали е валидна към момента;

1.3.11. има ли подадени жалби, сигнали, уведомления в КЗЛД и откази от съдействие, издадените АУАН и НП;

1.4. събиране на документи за изясняване на факти и обстоятелства по предмета на самосезирането:

1.4.1. проучване на приложимото към казуса законодателство и Насоките на Европейския комитет по защита на данните;

1.4.2.проучване на приложима към казуса практика – на КЗЛД, на Съда на Европейския съюз;

1.4.3. справки в публични бази данни;

1.4.4. справки в интернет страници;

1.4.5. телефонни разговори;

1.4.6. електронни съобщения;

1.4.7. изискване на становище/становища;

1.4.8. искане на становище/становища (при необходимост);

1.4.9. изпращане на уведомително писмо до сертифицирания АЛД за проверката с приложен въпросник, включително и по електронен път.

1.5. анализ на събраните в хода на проверката документи, в т.ч. Насоките на Европейския комитет по защита на данните и решенията на Съда на Европейския съюз, приложими към казуса;

1.6. анализ на сключените договори с физически или юридически лица и наличието на клаузи, регламентиращи обработването на личните данни;

1.7. в зависимост от казуса и събраните документи следва:

1.7.1. да се изготви констативен акт, който да се докладва на КЗЛД със съответните предложения на служителя/ите. Констативният акт може да съдържа предложения за приемане при липса на нарушение, за извършване на проверка на място (с предложение за членовете на екипите за проверки и привличане на външен експерт при

необходимост), за издаване на корективна мярка по чл. 58, § 2 от Регламент (ЕС) 2016/679, за препращане на събраната документация на друг компетентен орган, включително по Информационната система на вътрешния пазар и др.;

1.7.2. да се състави АУАН/НП само на база на събрани документи, без проверка на място, като задължително служителите на дирекция „ПАИКД“ следва да предприемат действия за потвърждение на фактите и обстоятелствата, съдържащи се в документите и събирането на допълнителни писмени материали, с оглед упражняването на правомощията на КЗЛД.

2. Проверки на място на сертифицирания АЛД – дирекция „ПАИКД“

2.1 Неприсъствени действия / Планиране / Предварителна подготовка:

2.1.1. приемане на решение на КЗЛД за извършване на проверка на място с определяне на предмета, обхвата и целите на проверката, включително привличане на външен експерт (при необходимост);

2.1.2. издаване на заповед за проверка с определяне на екипа за проверка – два оригинала;

2.1.3. изпращане на уведомително писмо за проверката до сертифицирания АЛД с приложен въпросник, включително и по електронен път.

2.2. Проверка на място в седалището/обект на сертифицирания АЛД:

2.2.1. легитимиране на проверяващия екип със служебни карти;

2.2.2. легитимация на сертифицирания АЛД;

2.2.3. връчване на заповедта на председателя на КЗЛД за извършване на проверката – връчва се оригинал на заповедта, като на екземпляра на проверяващия екип сертифицирания АЛД или упълномощеното от него лице собственоръчно написва текст, че е получил копие от заповедта за проверка, датата, трите си имена и подпис (за юридическите лица – печат, при възможност);

2.2.4. проверка за законосъобразно обработване на лични данни съобразно предмета и задачата на проверката;

2.2.5. задължителна проверка и събиране на доказателства относно:

а) дейността на сертифицирания АЛД – събиране на документация и доказателства, кореспондиращи с предварителното проучване на сертифицирания АЛД;

б) спазване принципите за законосъобразно обработване на лични данни (чл. 5, 6 от Регламент (ЕС) 2016/679);

в) условията за даване на съгласие (чл. 7 от Регламент (ЕС) 2016/679);

г) условията, приложими за съгласието на дете във връзка с услугите на информационното общество (чл. 8 от Регламент (ЕС) 2016/679);

д) обработването на специални категории лични данни (чл. 9 от Регламент (ЕС) 2016/679);

е) предприетите от сертифицирания АЛД действия за информиране на физическите лица за целите на обработване на личните им данни и упражняването на техните права съгласно чл. 15–22 от Регламент (ЕС) 2016/679;

ж) предаване на лични данни на трети държави или международни организации (чл. 44–50 от Регламент (ЕС) 2016/679) − на кои, основанието и начин на предаване, категории лични данни, технически и организационни мерки за защита;

з) обмен на лични данни с български институции – на кои, основанието и начин на предаване, категории лични данни, технически и организационни мерки за защита;

и) предприетите технически и организационни мерки за защита на личните данни;

й) наличие на одити по отношение спазването на Наредбата за минимални изисквания за мрежова и информационна сигурност и ISO 27701;

к) проверка на сигурността и сертифициране на информационните системи, обработващи лични данни;

л) наличие на сертификати за информационна сигурност и за защита на личните данни.

2.2.6. присъединил ли се е сертифицираният АЛД към одобрен кодекс за поведение (ако е относимо);

2.2.7. събиране на доказателства за всеки установен факт – документи на хартиен и/или електронен носител (в т.ч. направения анализ на риска и определяне на нивото на въздействие, правила, процедури, становища, екранни разпечатки и др.), като задължително сертифицирания АЛД предоставя заверени копия на сключени договори с физически или юридически лица, касаещи обработването на лични данни;

2.2.8. изготвяне на констативен протокол по време на проверката, екземпляр се връчва на сертифицирания АЛД;

2.2.9. изготвяне на приемо-предавателен протокол със заверени копия на документи и предоставени доказателства от сертифицирания АЛД, екземпляр се връчва на сертифицирания АЛД;

2.2.10. указване на срок за предоставяне на допълнителни документи (при необходимост).

3. Приключване на проверката

3.1. изготвяне на констативен акт и завеждането му в деловодната система, ведно с приложените в оригинал документи и доказателства, като задължително включва мнение и предложения на проверяващия екип:

3.1.1. предложение за приемане при липса на нарушение;

3.1.2. предложение за издаване на корективна мярка по чл. 58, § 2 от Регламент (ЕС) 2016/679;

3.1.3. при установяване на административно нарушение – предложение за налагане на санкция на сертифицирания АЛД, със стартиране на производство по ЗАНН със съставяне и връчване на АУАН.

4. Последващи действия на КЗЛД

4.1. приемане с Решение на изготвения констативен акт;

4.2. изготвяне на писмо до сертифицирания АЛД с констатации от проверката (когато няма наложена корективна мярка);

4.3. при издаване на корективна мярка по чл. 58, § 2 от Регламент (ЕС) 2016/679:

4.3.1. Решение на КЗЛД - диспозитивът на Решението задължително съдържа издадената корективна мярка (разпореждане), срок за нейното изпълнение, срок за представяне на доказателства за изпълнението му от сертифицирания АЛД, информация за административно-наказателната отговорност, която носи сертифицираниятАЛД в случай, че не го изпълни или не изпрати доказателства за изпълнението му в указания срок, както и за възможността за обжалване пред съответния съд;

4.3.2. Решението се връчва на сертифицирания АЛД;

4.3.3. след изтичане на 14-дневен срок влиза в сила и подлежи на изпълнение, ако ответната страна не оспорва Решението;

4.3.4. предоставяне на писмени доказателства от сертифицирания АЛД за изпълнение на корективната мярка и докладване на заседание на КЗЛД;

4.3.5. ако в указания срок сертифицираният АЛД не представи доказателства за изпълнение на корективната мярка:

а) изпраща се напомнително писмо с обратна разписка с указан 7-дневен срок, в който сертифицирания АЛД следва да предостави доказателства и/или становище за изпълнение на решението на КЗЛД и нейните разпореждания, както и информация за административно-наказателната отговорност, която носи сертифицираният АЛД в случай, че не го изпълни;

б) при изпълнение на указаното с писмото, се изготвя докладна записка до КЗЛД с предложение за приемане;

в) в случай на неизпълнение на указаното с писмото, се изготвя докладна записка до КЗЛД с предложение за налагане на административна санкцияпо реда на чл. 83, § 6 от Регламент (ЕС) 2016/679 и чл. 84 от ЗЗЛД, която се докладва на КЗЛД;

г) вземане на Решение на КЗЛД;

4.3.6. при прилагане на корективна мярка по чл. 58, § 2, буква „з“ от Регламент (ЕС) 2016/679 *(„…да разпореди на сертифициращия орган да отнеме сертификат.....“)*, се уведомява съответния СО;

4.4. издадените констативни актове се присъединяват към преписката;

4.5. издадените АУАН, НП и решенията за корективни мерки по чл. 58, § 2 от Регламент (ЕС) 2016/679 се вписват и съхраняват в съответния регистър.

В. Секторни/планови проверки на сертифицирани АЛД

1. Неприсъствени действия / Планиране / Предварителна подготовка

1.1. изготвяне на докладна записка с предложение за вземане на Решение на КЗЛД за извършване на планова проверка на сертифицирани АЛД на база на следните критерии:

1.1.1. обществена значимост на нарушенията, сигнализирани с жалби и сигнали;

1.1.2. повтаряемост на нарушенията;

1.1.3. промяна на законодателството;

1.1.4. други…….

1.2. докладната записка се внася за разглеждане и приемане на заседание на КЗЛД;

1.3. приемане на Решение на КЗЛД за извършване на планова проверка с определяне на предмета, обхвата, субектите и целите на проверката, вкл. привличане на външен експерт (при необходимост).

2. Проверки по документи

2.1. анализ на сертифицираните АЛД, на които ще бъде извършена проверка, по горепосочените критерии / предварително проучване на сертифицираните АЛД:

2.1.1. кой е СО, издал сертификата;

2.1.2. проверка дали сертифицирания АЛД отговаря на критериите, визирани в Наредба на КЗЛД по чл. 14, ал. 6 от ЗЗЛД;

2.1.3. проверка относно обхвата/предмета на сертифициране;

2.1.4. оценка на схемата за сертификация;

2.1.5. проверка на разпределение на нива и отговорности;

2.1.6. проверка на цялата релевантна документация;

2.1.7. на какъв период се извършва проверка от страна на СО, както и документацията, обективираща резултатите от тази проверка;

2.1.8. проверка за това дали се съблюдават стандартите ISO тогава, когато това е приложимо;

2.1.9. за какъв период е сертификацията и дали е валидна към момента;

2.1.10. има ли подадени жалби, сигнали, уведомления в КЗЛД и откази от съдействие, издадените АУАН и НП.

2.2. проучване на приложимото към казуса законодателство и Насоките на Европейския комитет по защита на данните;

2.3. проучване на приложима към казуса практика – на КЗЛД, на Съда на Европейския съюз;

2.4. справки в публични бази данни;

2.5. справки в интернет страници;

2.6. телефонни разговори;

2.7. електронни съобщения;

2.8. изискване на становище/становища;

2.9. искане на становище/становища (при необходимост);

2.10. изпращане на уведомително писмо за проверката до сертифицираните АЛД с приложен въпросник, включително и по електронен път;

2.11. анализ на събраните в хода на проверката документи, в т.ч. Насоките на Европейския комитет по защита на данните и решенията на Съда на Европейския съюз, приложими към казуса;

2.12. анализ на сключените договори с физически или юридически лица и наличието на клаузи, регламентиращи обработването на личните данни;

2.13. изготвяне на констативен акт за всеки сертифициран АЛД със предложение за приемане при липса на нарушение, за извършване на проверка на място (с предложение за членовете на екипите за проверки и привличане на външен експерт при необходимост), за издаване на корективна мярка по чл. 58, § 2 от Регламент (ЕС) 2016/679, за препращане на събраната документация на друг компетентен орган, включително по Информационната система на вътрешния пазар и др.;

2.14. констативните актове се внасят за разглеждане и приемане на заседание на КЗЛД;

2.15. при констатирано нарушение се изготвя АУАН/НП само на база на събрани документи, без проверка на място, като задължително служителите на дирекция „ПАИКД“ следва да предприемат действия за потвърждение на фактите и обстоятелствата, съдържащи се в документите и събирането на допълнителни писмени материали, с оглед упражняването на правомощията на КЗЛД.

3. Проверки на място на сертифицирани АЛД – дирекция „ПАИКД“

3.1. Неприсъствени действия / Планиране / Предварителна подготовка

3.1.1. приемане на Решение на КЗЛД за извършване на проверка с определяне на предмета, обхвата, субектите и целите на проверката, вкл. привличане на външен експерт (при необходимост);

3.1.2. издаване на заповед за проверка с определяне на екипа за проверка – два оригинала;

3.1.3. разписване на функции и отговорности на членовете на екипите за проверки;

3.1.4. изготвяне на хронограма за действията на екипа (при необходимост);

3.1.5. изпращане на уведомително писмо за проверката до всички сертифицирани АЛД с приложен въпросник, включително и по електронен път.

3.2. Проверка на място в седалището/обект на сертифицирани АЛД

3.2.1. легитимиране на проверяващия екип със служебни карти;

3.2.2. легитимация на сертифицирания АЛД;

3.2.3. връчване на заповедта на председателя на КЗЛД за извършване на проверката – връчва се оригинал на заповедта, като на екземпляра на проверяващия екип сертифицирания АЛД или упълномощеното от него лице собственоръчно написва текст, че е получил копие от заповедта за проверка, датата, трите си имена и подпис (за юридическите лица – печат, при възможност);

3.2.4. проверка за законосъобразно обработване на лични данни съобразно предмета и задачата на проверката;

3.2.5. задължителна проверка и събиране на доказателства относно:

а) дейността на сертифицирания АЛД – събиране на документация и доказателства, кореспондиращи с предварителното проучване на сертифицирания АЛД;

б) спазване принципите за законосъобразно обработване на лични данни (чл. 5, 6 от Регламент (ЕС) 2016/679);

в) условията за даване на съгласие (чл. 7 от Регламент (ЕС) 2016/679);

г) условията, приложими за съгласието на дете във връзка с услугите на информационното общество (чл. 8 от Регламент (ЕС) 2016/679);

д) обработването на специални категории лични данни (чл. 9 от Регламент (ЕС) 2016/679);

е) предприетите от сертифицирания АЛД действия за информиране на физическите лица за целите на обработване на личните им данни и упражняването на техните права съгласно чл. 15–22 от Регламент (ЕС) 2016/679;

ж) предаване на лични данни на трети държави или международни организации (чл. 44–50 от Регламент (ЕС) 2016/679) − на кои, основанието и начин на предаване, категории лични данни, технически и организационни мерки за защита;

з) обмен на лични данни с български институции – на кои, основанието и начин на предаване, категории лични данни, технически и организационни мерки за защита;

и) предприетите технически и организационни мерки за защита на личните данни;

й) наличие на одити по отношение спазването на Наредбата за минимални изисквания за мрежова и информационна сигурност и ISO 27701;

к) проверка на сигурността и сертифициране на информационните системи, обработващи лични данни;

л) наличие на сертификати за информационна сигурност и за защита на личните данни.

3.2.6. присъединил ли се е сертифицираният АЛД към одобрен кодекс за поведение (ако е относимо към проверката);

3.2.7. събиране на доказателства за всеки установен факт – документи на хартиен и/или електронен носител (в т.ч. направения анализ на риска и определяне на нивото на въздействие, правила, процедури, становища, екранни разпечатки и др.), като задължително сертифицираният АЛД предоставя заверени копия на сключени договори с физически или юридически лица, касаещи обработването на лични данни;

3.2.8. изготвяне на констативен протокол по време на проверката, екземпляр се връчва на сертифицирания АЛД;

3.2.9. изготвяне на приемо-предавателен протокол със заверени копия на документи и предоставени доказателства от сертифицирания АЛД, екземпляр се връчва на сертифицирания АЛД;

3.2.10. указване на срок за предоставяне на допълнителни документи (при необходимост).

3.3. Приключване на проверката на място:

3.3.1. изготвяне на констативен акт и завеждането му в деловодната система, ведно с приложените в оригинал документи и доказателства, като задължително включва мнение и предложения на проверяващия екип:

а) предложение за приемане при липса на нарушение;

б) предложение за издаване на корективна мярка по чл. 58, § 2 от Регламент (ЕС) 2016/679;

в) при установяване на административно нарушение – предложение за налагане на санкция на сертифицирания АЛД, със стартиране на производство по ЗАНН със съставяне и връчване на АУАН;

3.3.2. констативният акт се внася за разглеждане и приемане на заседание на КЗЛД.

4. Приключване на Секторната проверка / Плановата проверка / Одита

4.1. изготвяне на окончателен доклад за Секторната проверка / Плановата проверка / Одита, съдържащ обобщен анализ на извършените проверки (по документи и на място), заключения и предложения до КЗЛД за изготвяне на препоръки към всички сертифицирани АЛД (при необходимост);

4.2. внасяне за разглеждане и приемане на окончателния доклад на заседание на КЗЛД.

5. Последващи действия на КЗЛД

5.1. приемане с решение на изготвените констативни актове;

5.2. запознаване и приемане на окончателния доклад за Секторната проверка / Плановата проверка / Одита и одобрение на препоръки към всички сертифицирани АЛД (при необходимост);

5.3. публикуване на анонимизиран окончателен доклад и препоръките на интернет страницата на КЗЛД;

5.4. изготвяне на писмо до съответните сертифицирани АЛД с констатации от проверката (когато няма наложена корективна мярка);

5.5. при издаване на корективна мярка по чл. 58, § 2 от Регламент (ЕС) 2016/679

5.5.1 Решение на КЗЛД − диспозитивът на Решението задължително съдържа издадената корективна мярка (разпореждане), срок за нейното изпълнение, срок за представяне на доказателства за изпълнението му от сертифицирания АЛД, информация за административно-наказателната отговорност, която носи сертифицираниятАЛД в

случай, че не го изпълни или не изпрати доказателства за изпълнението му в указания срок, както и за възможността за обжалване пред съответния съд;

5.5.2. Решението се връчва на сертифицирания АЛД;

5.5.3. след изтичане на 14-дневен срок влиза в сила и подлежи на изпълнение, ако ответната страна не оспорва Решението;

5.5.4. предоставяне на писмени доказателства от сертифицирания АЛД за изпълнение на корективната мярка и докладване на заседание на КЗЛД;

5.5.5. ако в указания срок сертифицирания АЛД не представи доказателства за изпълнение на корективната мярка

а) изпраща се напомнително писмо с обратна разписка с указан 7-дневен срок, в който сертифицираният АЛД следва да предостави доказателства и/или становище за изпълнение на решението на КЗЛД и нейните разпореждания, както и информация за административно-наказателната отговорност, която носи сертифицираният АЛД в случай, че не го изпълни;

б) при изпълнение на указаното с писмото, се изготвя докладна записка до КЗЛД с предложение за приемане;

в) в случай на неизпълнение на указаното с писмото, се изготвя докладна записка до КЗЛД с предложение за налагане на административна санкцияпо реда на чл. 83, § 6 от Регламент (ЕС) 2016/679 и чл. 84 от ЗЗЛД, която се докладва на КЗЛД;

г) вземане на Решение на КЗЛД.

5.5.6. при прилагане на корективна мярка по чл. 58, § 2, буква „з“ от Регламент (ЕС) 2016/679 *(„…да разпореди на сертифициращия орган да отнеме сертификат.....“)*, се уведомява съответния сертифициран АЛД.

5.6. издадените констативни актове се присъединяват към преписката;

5.7. издадените АУАН, НП и решенията за корективни мерки по чл. 58, § 2 от Регламент (ЕС) 2016/679 се вписват и съхраняват в съответния регистър.

X. ПРОВЕРКИ НА ОРГАНИ ЗА НАБЛЮДЕНИЕ НА КОДЕКСИ ЗА ПОВЕДЕНИЕ (ОН) – ДИРЕКЦИЯ „ПАИКД“

А. Проверки след подаден сигнал

1. Проверки по документи

1.1. входиране на сигнал в деловодството на КЗЛД;

1.2. определяне на служител / екип от служители за разглеждането на сигнала;

1.3. проверка дали ОН фигурира в регистъра на КЗЛД;

1.4. предварително проучване на ОН:

1.4.1. проверка от кого е акредитиран органа за наблюдение на кодекс за поведение и дали продължава да отговаря на критериите за акредитация, съгласно Наредба на КЗЛД по чл. 14а, ал. 3 от ЗЗЛД;

1.4.2. проверка на срока на акредитацията;

1.4.3. проверка колко АЛД/ОЛД са присъединени към кодекса и дали са обхванати от органа на наблюдение, с приложени доказателства;

1.4.4. проверка относно осъществяването на надзора, който ОН прилага върху присъединените към кодекса – спазването на предвидените в кодекса процедури. Прилагане на доказателства;

1.4.5. доказателства за прилагането на процедура за недопустимост на конфликт на интереси, безпристрастност;

1.4.6. продължават ли да са налице достатъчно ресурси за осъществяването на дейността по наблюдение;

1.4.7. има ли подадени жалби, сигнали, уведомления в КЗЛД и откази от съдействие, издадените АУАН и НП.

1.5. проучване на приложимото към казуса законодателство и Насоките на Европейския комитет по защита на данните;

1.6. проучване на приложима към казуса практика – на КЗЛД, на Съда на Европейския съюз;

1.7. справки в публични бази данни;

1.8. справки в интернет страници;

1.9. телефонни разговори;

1.10. електронни съобщения;

1.11. изискване на становище/становища;

1.12. искане на становище/становища (при необходимост);

1.13. анализ на събраните в хода на проверката документи, в т.ч. Насоките на Европейския комитет по защита на данните и решенията на Съда на Европейския съюз, приложими към казуса;

1.14. анализ на сключените договори с физически или юридически лица и наличието на клаузи, регламентиращи обработването на личните данни;

1.15. изготвяне на отговор до сигналоподателя, без да се предприемат последващи действия;

1.16. сигналът да се препрати по компетентност на друг орган/органи;

1.17. в зависимост от казуса на сигнала и събраните документи следва:

1.17.1. да се изготви констативен акт, който да се докладва на КЗЛД със съответните предложения на служителя, разглеждащ сигнала. Констативният акт може да съдържа предложения за приемане при липса на нарушение, за преквалифицирането на сигнала в жалба, за отнемане на акредитацията, за извършване на проверка на място (с предложение за членовете на екипите за проверки и привличане на външен експерт при необходимост), за издаване на корективна мярка по чл. 58, § 2 от Регламент (ЕС) 2016/679, за препращане на събраната документация на друг компетентен орган, включително по Информационната система на вътрешния пазар и др.;

1.17.2 да се състави АУАН/НП само на база на събрани документи, без проверка на място, като задължително служителите на дирекция „ПАИКД“ следва да предприемат действия за потвърждение на фактите и обстоятелствата, съдържащи се в документите и събирането на допълнителни писмени материали, с оглед упражняването на правомощията на КЗЛД.

1.18. при получаване на документи, изпратени по компетентност на КЗЛД от Прокуратурата на Република България / МВР и други органи:

1.18.1. препращане по компетентност на друг орган/органи;

1.18.2. издаване на корективна мяркапо чл. 58, § 2 от Регламент (ЕС) 2016/679;

1.18.3. стартиране на процедура по ЗАНН със съставяне на АУАН по документи, като служителите на дирекция „ПАИКД“ следва задължително да предприемат действия за потвърждение на фактите и обстоятелствата, съдържащи се в документите и събирането на допълнителни писмени материали, с оглед упражняването на правомощията на КЗЛД.

1.19. изготвяне на отговор до сигналоподателя, съдържащ информация за предприетите от КЗЛД действия, с препращане към друг орган / издаване на корективна мярка / налагане на санкция.

2. Проверки на място на ОН – дирекция „ПАИКД“

2.1. Неприсъствени действия / Планиране / Предварителна подготовка:

2.1.1. приемане на Решение на КЗЛД за извършване на проверка на място;

2.1.2. издаване на заповед за проверка с определяне на екипа за проверка, предмета, обхвата и целите на проверката, включително привличане на външен експерт (при необходимост) – два оригинала;

2.1.3. изпращане на уведомително писмо с въпросник (при необходимост), включително и по електронен път.

2.2. Проверка на място в седалището/обект на ОН:

2.2.1. легитимиране на проверяващия екип със служебни карти;

2.2.2. легитимация на представляващия ОН;

2.2.3. връчване на заповедта на председателя на КЗЛД за извършване на проверката – връчва се оригинал на заповедта, като на екземпляра на проверяващия екип представляващия ОН или упълномощеното от него лице собственоръчно написва текст, че е получил копие от заповедта за проверка, датата, трите си имена и подпис (за юридическите лица – печат, при възможност);

2.2.4. изясняване на факти и обстоятелства по отношение на получения сигнал;

2.2.5 проверка за законосъобразно обработване на лични данни съобразно предмета на сигнала и задачата на проверката;

2.2.6. изясняване на факти и обстоятелства по отношение на дейността на ОН – събиране на документация и доказателства, кореспондиращи с предварителното проучване на ОН;

2.2.7. наличие на одити по отношение спазването на Наредбата за минимални изисквания за мрежова и информационна сигурност и ISO 27701 (ако е относимо към предмета на сигнала);

2.2.8. проверка на сигурността и сертифициране на информационните системи, обработващи лични данни (ако е относимо към предмета на сигнала);

2.2.9. наличие на сертификати за информационна сигурност и за защита на личните данни (ако е относимо към предмета на сигнала);

2.2.10. присъединил ли се е ОН към одобрен кодекс за поведение (ако е относимо към предмета на сигнала);

2.2.11. събиране на доказателства за всеки установен факт – документи на хартиен и/или електронен носител (в т.ч. направения анализ на риска и определяне на нивото на въздействие, правила, процедури, становища, екранни разпечатки и др.), като задължително ОН предоставя заверени копия на сключени договори с физически или юридически лица, касаещи обработването на лични данни;

2.2.12. изготвяне на констативен протокол по време на проверката, екземпляр се връчва на ОН;

2.2.13. изготвяне на приемо-предавателен протокол със заверени копия на документи и предоставени доказателства от ОН, екземпляр се връчва на ОН;

2.2.14. указване на срок за предоставяне на допълнителни документи (при необходимост).

3. Приключване на проверката

3.1. изготвяне на констативен акт и завеждането му в деловодната система, ведно с приложените в оригинал документи и доказателства, като задължително включва мнение и предложения на проверяващия екип:

3.1.1. предложение за приемане при липса на нарушение;

3.1.2. предложение за отнемане на акредитацията;

3.1.3. предложение за издаване на корективна мярка по чл. 58, § 2 от Регламент (ЕС) 2016/679;

3.1.4. при установяване на административно нарушение – предложение за налагане на санкция на ОН, със стартиране на производство по ЗАНН със съставяне и връчване на АУАН.

4. Последващи действия на КЗЛД

4.1. приемане с Решение на изготвения констативен акт;

4.2. изготвяне на писмо до ОН с констатации от проверката (когато няма наложена корективна мярка);

4.3. при отнемане на акредитацията – на ОН се изпраща заверено копие на Решението на КЗЛД; уведомява се предложилия кодекса за поведение и се следва реда, разписан в Наредбата по чл. 14а, ал. 3 от ЗЗЛД;

4.4. при издаване на корективна мярка по чл. 58, § 2 от Регламент (ЕС) 2016/679:

4.4.1. Решение на КЗЛД - диспозитивът на Решението задължително съдържа издадената корективна мярка (разпореждане), срок за нейното изпълнение, срок за представяне на доказателства за изпълнението му от ОН, информация за административно-наказателната отговорност, която носи ОН в случай, че не го изпълни или не изпрати доказателства за изпълнението му в указания срок, както и за възможността за обжалване пред съответния съд;

4.4.2. Решението се връчва на съответния ОН;

4.4.3 след изтичане на 14-дневен срок влиза в сила и подлежи на изпълнение, ако ответната страна не оспорва Решението;

4.4.4. предоставяне на писмени доказателства от ОН за изпълнение на коративната мярка и докладване на заседание на КЗЛД;

4.4.5. ако в указания срок ОН не представи доказателства за изпълнение на коративната мярка:

а) изпраща се напомнително писмо с обратна разписка с указан 7-дневен срок, в който ОН следва да предостави доказателства и/или становище за изпълнение на

решението на КЗЛД и нейните разпореждания, както и информация за административно-наказателната отговорност, която носи ОН в случай, че не го изпълни;

б) при изпълнение на указаното с писмото, се изготвя докладна записка до КЗЛД с предложение за приемане;

в) в случай на неизпълнение на указаното с писмото, се изготвя докладна записка до КЗЛД с предложение за налагане на административна санкцияпо реда на чл. 83, § 6 от Регламент (ЕС) 2016/679 и чл. 84 от ЗЗЛД, която се докладва на КЗЛД;

г) вземане на Решение на КЗЛД.

4.5. издадените констативни актове се присъединяват към преписката;

4.6. издадените АУАН, НП и решенията за корективни мерки по чл. 58, § 2 от Регламент (ЕС) 2016/679 се вписват и съхраняват в съответния регистър.

Б. Проверки на ОН при висок обществен интерес / Самосезиране на КЗЛД

1. Проверки по документи

1.1. приемане на Решение на КЗЛД за самосезиране, в т.ч. при възникване на казус с висок обществен интерес;

1.2. определяне на служител / екип от служители за извършване на проверка по документи;

1.3. предварително проучване на ОН:

1.3.1. проверка дали ОН фигурира в регистъра на КЗЛД;

1.3.2. проверка дали акредитираният орган за наблюдение на кодекс за поведение продължава да отговаря на критериите за акредитация, съгласно Наредба на КЗЛД по чл. 14а, ал. 3 от ЗЗЛД;

1.3.3. проверка на срока на акредитацията;

1.3.4. проверка колко АЛД/ОЛД са присъединени към кодекса и дали са обхванати от органа на наблюдение, с приложени доказателства;

1.3.5. проверка относно осъществяването на надзора, който ОН прилага върху присъединените към кодекса – спазването на предвидените в кодекса процедури. Прилагане на доказателства;

1.3.6. доказателства за прилагането на процедура за недопустимост на конфликт на интереси, безпристрастност;

1.3.7. продължават ли да са налице достатъчно ресурси за осъществяването на дейността по наблюдение;

1.3.8. има ли подадени жалби, сигнали, уведомления в КЗЛД и откази от съдействие, издадените АУАН и НП.

1.4. събиране на документи за изясняване на факти и обстоятелства по предмета на самосезирането:

1.4.1. проучване на приложимото към казуса законодателство и Насоките на Европейския комитет по защита на данните;

1.4.2. проучване на приложима към казуса практика – на КЗЛД, на Съда на Европейския съюз;

1.4.3. справки в публични бази данни;

1.4.4. справки в интернет страници;

1.4.5. телефонни разговори;

1.4.6. електронни съобщения;

1.4.7. изискване на становище/становища;

1.4.8. искане на становище/становища (при необходимост);

1.4.9. изпращане на уведомително писмо за проверката до ОН с приложен въпросник, включително и по електронен път.

1.5. анализ на събраните в хода на проверката документи, в т.ч. Насоките на Европейския комитет по защита на данните и решенията на Съда на Европейския съюз, приложими към казуса;

1.6. анализ на сключените договори с физически или юридически лица и наличието на клаузи, регламентиращи обработването на личните данни;

1.7. в зависимост от казуса и събраните документи следва:

1.7.1. да се изготви констативен акт, който да се докладва на КЗЛД със съответните предложения на служителя/ите. Констативният акт може да съдържа предложения за приемане при липса на нарушение, за отнемане на акредитацията, за извършване на проверка на място (с предложение за членовете на екипите за проверки и привличане на външен експерт при необходимост), за издаване на корективна мярка по чл. 58, § 2 от Регламент (ЕС) 2016/679, за препращане на събраната документация на друг компетентен орган, включително по Информационната система на вътрешния пазар и др.;

1.7.2 да се състави АУАН/НП само на база на събрани документи, без проверка на място, като задължително служителите на дирекция „ПАИКД“ следва да предприемат действия за потвърждение на фактите и обстоятелствата, съдържащи се в документите и събирането на допълнителни писмени материали, с оглед упражняването на правомощията на КЗЛД.

2. Проверки на място на ОН – дирекция „ПАИКД“

2.1. Неприсъствени действия / Планиране / Предварителна подготовка:

2.1.1. приемане на решение на КЗЛД за извършване на проверка на място с определяне на предмета, обхвата и целите на проверката, включително привличане на външен експерт (при необходимост);

2.1.2. издаване на заповед за проверка с определяне на екипа за проверка – два оригинала;

2.1.3. изпращане на уведомително писмо за проверката до ОН с приложен въпросник, включително и по електронен път.

2.2. Проверка на място в седалището/обект на ОН:

2.2.1. легитимиране на проверяващия екип със служебни карти;

2.2.2. легитимация на представляващия ОН;

2.2.3. връчване на заповедта на председателя на КЗЛД за извършване на проверката – връчва се оригинал на заповедта, като на екземпляра на проверяващия екип представляващия ОН или упълномощеното от него лице собственоръчно написва текст, че е получил копие от заповедта за проверка, датата, трите си имена и подпис (за юридическите лица – печат, при възможност);

2.2.4. проверка за законосъобразно обработване на лични данни съобразно предмета и задачата на проверката;

2.2.5. задължителна проверка и събиране на доказателства относно:

а) дейността на ОН – събиране на документация и доказателства, кореспондиращи с предварителното проучване на ОН;

б) присъединил ли се е ОН към одобрен кодекс за поведение (ако е относимо);

в) събиране на доказателства за всеки установен факт – документи на хартиен и/или електронен носител (в т.ч. направения анализ на риска и определяне на нивото на въздействие, правила, процедури, становища, екранни разпечатки и др.), като задължително ОН предоставя заверени копия на сключени договори с физически или юридически лица, касаещи обработването на лични данни;

2.2.6. в случай, че е относимо към проверката, събиране на доказателства относно:

а) спазване принципите за законосъобразно обработване на лични данни (чл. 5, 6 от Регламент (ЕС) 2016/679);

б) условията за даване на съгласие (чл. 7 от Регламент (ЕС) 2016/679);

в) условията, приложими за съгласието на дете във връзка с услугите на информационното общество (чл. 8 от Регламент (ЕС) 2016/679);

г) обработването на специални категории лични данни (чл. 9 от Регламент (ЕС) 2016/679);

д) предприетите от ОН действия за информиране на физическите лица за целите на обработване на личните им данни и упражняването на техните права съгласно чл. 15–22 от Регламент (ЕС) 2016/679;

е) предаване на лични данни на трети държави или международни организации (чл. 44–50 от Регламент (ЕС) 2016/679) − на кои, основанието и начин на предаване, категории лични данни, технически и организационни мерки за защита;

ж) обмен на лични данни с български институции – на кои, основанието и начин на предаване, категории лични данни, технически и организационни мерки за защита;

з) предприетите технически и организационни мерки за защита на личните данни;

и) наличие на одити по отношение спазването на Наредбата за минимални изисквания за мрежова и информационна сигурност и ISO 27701;

й) проверка на сигурността и сертифициране на информационните системи, обработващи лични данни;

к) наличие на сертификати за информационна сигурност и за защита на личните данни.

2.2.7 изготвяне на констативен протокол по време на проверката, екземпляр се връчва на ОН;

2.2.8. изготвяне на приемо-предавателен протокол със заверени копия на документи и предоставени доказателства от ОН, екземпляр се връчва на ОН;

2.2.9. указване на срок за предоставяне на допълнителни документи (при необходимост).

3. Приключване на проверката

3.1. изготвяне на констативен акт и завеждането му в деловодната система, ведно с приложените в оригинал документи и доказателства, като задължително включва мнение и предложения на проверяващия екип:

3.1.1. предложение за приемане при липса на нарушение;

3.1.2. предложение за отнемане на акредитацията;

3.1.3. предложение за издаване на корективна мярка по чл. 58, § 2 от Регламент (ЕС) 2016/679;

3.1.4. при установяване на административно нарушение – предложение за налагане на санкция на ОН, със стартиране на производство по ЗАНН със съставяне и връчване на АУАН.

4. Последващи действия на КЗЛД

4.1. приемане с Решение на изготвения констативен акт;

4.2. изготвяне на писмо до ОН с констатации от проверката (когато няма наложена корективна мярка);

4.3. при отнемане на акредитацията – на ОН се изпраща заверено копие на Решението на КЗЛД; уведомява се предложилия кодекса за поведение и се следва реда, разписан в Наредбата по чл. 14а, ал. 3 от ЗЗЛД;

4.4. при издаване на корективна мярка по чл. 58, § 2 от Регламент (ЕС) 2016/679

4.4.1. Решение на КЗЛД - диспозитивът на Решението задължително съдържа издадената корективна мярка (разпореждане), срок за нейното изпълнение, срок за представяне на доказателства за изпълнението му от ОН, информация за административно-наказателната отговорност, която носи ОН в случай, че не го изпълни или не изпрати доказателства за изпълнението му в указания срок, както и за възможността за обжалване пред съответния съд;

4.4.2. Решението се връчва на съответния ОН;

4.4.3. след изтичане на 14-дневен срок влиза в сила и подлежи на изпълнение, ако ответната страна не оспорва Решението;

4.4.4. предоставяне на писмени доказателства от ОН за изпълнение на коративната мярка и докладване на заседание на КЗЛД;

4.4.5. ако в указания срок ОН не представи доказателства за изпълнение на коративната мярка:

а) изпраща се напомнително писмо с обратна разписка с указан 7-дневен срок, в който ОН следва да предостави доказателства и/или становище за изпълнение на решението на КЗЛД и нейните разпореждания, както и информация за административно-наказателната отговорност, която носи ОН в случай, че не го изпълни;

б) при изпълнение на указаното с писмото, се изготвя докладна записка до КЗЛД с предложение за приемане;

в) в случай на неизпълнение на указаното с писмото, се изготвя докладна записка до КЗЛД с предложение за налагане на административна санкцияпо реда на чл. 83, § 6 от Регламент (ЕС) 2016/679 и чл. 84 от ЗЗЛД, която се докладва на КЗЛД;

г) вземане на Решение на КЗЛД.

4.5. издадените констативни актове се присъединяват към преписката;

4.6. издадените АУАН, НП и решенията за корективни мерки по чл. 58, § 2 от Регламент (ЕС) 2016/679 се вписват и съхраняват в съответния регистър.

В. Секторни провеки / Планови проверки / Одити на ОН

1. Неприсъствени действия / Планиране / Предварителна подготовка

1.1. изготвяне на докладна записка с предложение за вземане на Решение на КЗЛД за извършване на планова проверка на ОН на база на следните критерии:

1.1.1. обществена значимост на нарушенията, сигнализирани с жалби и сигнали;

1.1.2. повтаряемост на нарушенията;

1.1.3. промяна на законодателството;

1.1.4. други…….

1.2. докладната записка се внася за разглеждане и приемане на заседание на КЗЛД;

1.3. приемане на Решение на КЗЛД за извършване на планова проверка с определяне на предмета, обхвата, субектите и целите на проверката, вкл. привличане на външен експерт (при необходимост).

2. Проверки по документи

2.1. анализ на ОН, на които ще бъде извършена проверка, по горепосочените критерии / предварително проучване на ОН:

2.1.1. проверка дали ОН фигурира в регистъра на КЗЛД;

2.1.2. проверка дали акредитираният орган за наблюдение на кодекс за поведение продължава да отговаря на критериите за акредитация, съгласно Наредба на КЗЛД по чл. 14а, ал. 3 от ЗЗЛД;

2.1.3. проверка на срока на акредитацията;

2.1.4. проверка колко АЛД/ОЛД са присъединени към кодекса и дали са обхванати от органа на наблюдение, с приложени доказателства;

2.1.5. проверка относно осъществяването на надзора, който ОН прилага върху присъединените към кодекса – спазването на предвидените в кодекса процедури. Прилагане на доказателства;

2.1.6. доказателства за прилагането на процедура за недопустимост на конфликт на интереси, безпристрастност;

2.1.7. продължават ли да са налице достатъчно ресурси за осъществяването на дейността по наблюдение;

2.1.8. има ли подадени жалби, сигнали, уведомления в КЗЛД и откази от съдействие, издадените АУАН и НП.

2.2. проучване на приложимото към казуса законодателство и Насоките на Европейския комитет по защита на данните;

2.3. проучване на приложима към казуса практика – на КЗЛД, на Съда на Европейския съюз;

2.4. справки в публични бази данни;

2.5. справки в интернет страници;

2.6. телефонни разговори;

2.7. електронни съобщения;

2.8. изискване на становище/становища;

2.9. искане на становище/становища (при необходимост);

2.10. изпращане на уведомително писмо за проверката до всички ОН с приложен въпросник, включително и по електронен път;

2.11. анализ на събраните в хода на проверката документи, в т.ч. Насоките на Европейския комитет по защита на данните и решенията на Съда на Европейския съюз, приложими към казуса;

2.12. анализ на сключените договори с физически или юридически лица и наличието на клаузи, регламентиращи обработването на личните данни;

2.13. изготвяне на констативен акт за всеки ОН със предложение за приемане при липса на нарушение, за отнемане на акредитацията, за извършване на проверка на място (с предложение за членовете на екипите за проверки и привличане на външен експерт при необходимост), за издаване на корективна мярка по чл. 58, § 2 от Регламент (ЕС) 2016/679, за препращане на събраната документация на друг компетентен орган, включително по Информационната система на вътрешния пазар и др.;

2.14 констативните актове се внасят за разглеждане и приемане на заседание на КЗЛД;

2.15. при констатирано нарушение се изготвя АУАН/НП само на база на събрани документи, без проверка на място, като задължително служителите на дирекция „ПАИКД“ следва да предприемат действия за потвърждение на фактите и обстоятелствата, съдържащи се в документите и събирането на допълнителни писмени материали, с оглед упражняването на правомощията на КЗЛД.

3. Проверки на място на ОН – дирекция „ПАИКД“

3.1. Неприсъствени действия / Планиране / Предварителна подготовка:

3.1.1. приемане на Решение на КЗЛД за извършване на проверка с определяне на предмета, обхвата, субектите и целите на проверката, вкл. привличане на външен експерт (при необходимост);

3.1.2. издаване на заповед за проверка с определяне на екипа за проверка – два оригинала;

3.1.3. разписване на функции и отговорности на членовете на екипите за проверки;

3.1.4. изготвяне на хронограма за действията на екипа (при необходимост);

3.1.5. изпращане на уведомително писмо за проверката до всички ОН с приложен въпросник, включително и по електронен път.

3.2. Проверки на място в седалището/обект на ОН

3.2.1. легитимиране на проверяващия екип със служебни карти;

3.2.2. легитимация на представляващия ОН;

3.2.3. връчване на заповедта на председателя на КЗЛД за извършване на проверката – връчва се оригинал на заповедта, като на екземпляра на проверяващия екип представляващия ОН или упълномощеното от него лице собственоръчно написва текст, че е получил копие от заповедта за проверка, датата, трите си имена и подпис (за юридическите лица – печат, при възможност);

3.2.4. проверка за законосъобразно обработване на лични данни съобразно предмета и задачата на проверката (ако е относимо към проверката);

3.2.5. задължителна проверка и събиране на доказателства относно:

а) дейността на ОН – събиране на документация и доказателства, кореспондиращи с предварителното проучване на ОН;

б) наличие на одити по отношение спазването на Наредбата за минимални изисквания за мрежова и информационна сигурност и ISO 27701;

в) проверка на сигурността и сертифициране на информационните системи, обработващи лични данни;

г) наличие на сертификати за информационна сигурност и за защита на личните данни.

3.2.6. в случай, че е относимо към проверката, събиране на доказателства относно:

а) спазване принципите за законосъобразно обработване на лични данни (чл. 5, 6 от Регламент (ЕС) 2016/679);

б) условията за даване на съгласие (чл. 7 от Регламент (ЕС) 2016/679);

в) условията, приложими за съгласието на дете във връзка с услугите на информационното общество (чл. 8 от Регламент (ЕС) 2016/679);

г) обработването на специални категории лични данни (чл. 9 от Регламент (ЕС) 2016/679);

д) предприетите от ОН действия за информиране на физическите лица за целите на обработване на личните им данни и упражняването на техните права съгласно чл. 15–22 от Регламент (ЕС) 2016/679;

е) предаване на лични данни на трети държави или международни организации (чл. 44–50 от Регламент (ЕС) 2016/679) − на кои, основанието и начин на предаване, категории лични данни, технически и организационни мерки за защита;

ж) обмен на лични данни с български институции – на кои, основанието и начин на предаване, категории лични данни, технически и организационни мерки за защита;

з) предприетите технически и организационни мерки за защита на личните данни.

3.2.7. присъединил ли се е ОН към одобрен кодекс за поведение (ако е относимо);

3.2.8. събиране на доказателства за всеки установен факт – документи на хартиен и/или електронен носител (в т.ч. направения анализ на риска и определяне на нивото на въздействие, правила, процедури, становища, екранни разпечатки и др.), като задължително ОН предоставя заверени копия на сключени договори с физически или юридически лица, касаещи обработването на лични данни;

3.2.9. изготвяне на констативен протокол по време на проверката, екземпляр се връчва на ОН;

3.2.10. изготвяне на приемо-предавателен протокол със заверени копия на документи и предоставени доказателства от ОН, екземпляр се връчва на ОН;

3.2.11. указване на срок за предоставяне на допълнителни документи (при необходимост).

3.3. Приключване на проверката на място:

3.3.1. изготвяне на констативен акт и завеждането му в деловодната система, ведно с приложените в оригинал документи и доказателства, като задължително включва мнение и предложения на проверяващия екип:

а) предложение за приемане при липса на нарушение;

б) предложение за отнемане на акредитацията;

в) предложение за издаване на корективна мярка по чл. 58, § 2 от Регламент (ЕС) 2016/679;

г) при установяване на административно нарушение – предложение за налагане на санкция на ОН, със стартиране на производство по ЗАНН със съставяне и връчване на АУАН;

3.3.2. приемане с Решение на КЗЛД на изготвените констативни актове.

4. Приключване на Секторната проверка / Плановата проверка / Одита

4.1. изготвяне на окончателен доклад за Секторната проверка / Плановата проверка / Одита, съдържащ анализ, заключения и предложение до КЗЛД за изготвяне на препоръки към всички ОН (при необходимост);

4.2. внасяне на окончателния доклад за разглеждане и приемане на заседание на КЗЛД.

5. Последващи действия на КЗЛД

5.1. запознаване и приемане на окончателния доклад за Секторната проверка / Плановата проверка / Одита и одобрение на препоръки към всички ОН;

5.2. публикуване на анонимизиран окончателен доклад и препоръките на интернет страницата на КЗЛД;

5.3. изготвяне на писмо до съответните ОН с констатации от проверката (когато няма наложена корективна мярка);

5.4. при отнемане на акредитацията – на съответните ОН се изпраща заверено копие на Решението на КЗЛД; уведомява се предложилия кодекса за поведение и се следва реда, разписан в Наредбата по чл. 14а, ал. 3 от ЗЗЛД;

5.5. при издаване на корективна мярка по чл. 58, § 2 от Регламент (ЕС) 2016/679:

5.5.1. Решение на КЗЛД − диспозитивът на Решението задължително съдържа издадената корективна мярка (разпореждане), срок за нейното изпълнение, срок за представяне на доказателства за изпълнението му от ОН, информация за административно-наказателната отговорност, която носи ОН в случай, че не го изпълни или не изпрати доказателства за изпълнението му в указания срок, както и за възможността за обжалване пред съответния съд;

5.5.2. Решението се връчва на съответния ОН;

5.5.3. след изтичане на 14-дневен срок влиза в сила и подлежи на изпълнение, ако ответната страна не оспорва Решението;

5.5.4. предоставяне на писмени доказателства от ОН за изпълнение на корективната мярка и докладване на заседание на КЗЛД;

5.5.5. ако в указания срок ОН не представи доказателства за изпълнение на корективната мярка:

а) изпраща се напомнително писмо с обратна разписка с указан 7-дневен срок, в който ОН следва да предостави доказателства и/или становище за изпълнение на решението на КЗЛД и нейните разпореждания, както и информация за административно-наказателната отговорност, която носи ОН в случай, че не го изпълни;

б) при изпълнение на указаното с писмото, се изготвя докладна записка до КЗЛД с предложение за приемане;

в) в случай на неизпълнение на указаното с писмото, се изготвя докладна записка до КЗЛД с предложение за налагане на административна санкцияпо реда на чл. 83, § 6 от Регламент (ЕС) 2016/679 и чл. 84 от ЗЗЛД, която се докладва на КЗЛД;

г) вземане на Решение на КЗЛД.

5.6. издадените констативни актове се присъединяват към преписката;

5.7. издадените АУАН, НП и решенията за корективни мерки по чл. 58, § 2 от Регламент (ЕС) 2016/679 се вписват и съхраняват в съответния регистър.

XI. ОТКАЗ ОТ СЪДЕЙСТВИЕ

1. Определяне на отказа от съдействие

1.1. съгласно чл. 12а от ЗЗЛД – АЛД/ОЛД оказва съдействие на КЗЛД при изпълнение на нейните задачи и правомощия;

1.2. когато при упражняване на правомощията на КЗЛД по чл. 58, § 1, букви „д“ и „е“ от Регламент 2016/679 може да се наруши задължение на АЛД/ОЛД за опазване на професионална тайна или друго задължение за опазване на тайна, произтичащо от закон, АЛД/ОЛД могат да откажат предоставяне или достъп само до информацията, защитена като тайна;

1.3. когато информацията съдържа данни, представляващи класифицирана информация, се прилага редът за достъп по ЗЗКИ, като в проверката участват служители със съответното ниво на достъп;

1.4. във всички останали случай (неизпращане в указан срок на доказателства, документи, становища, отказ за осигуряване на достъп до помещенията и регистрите с лични данни на екип за извършване на проверка на място и др.) се съставя протокол за

отказ от съдействие се съставя протокол от служител на КЗЛД, подкрепен със съответните доказателства за бездействията/действията на АЛД/ОЛД;

1.5. протоколът се докладва на КЗЛД с предложение за стартиране на производство по ЗАНН;

1.6. събрани доказателства се прилагат по преписката с цел съставяне на АУАН и стартиране на АНП и издаване на НП, като санкцията се налага по реда на чл. 85, ал. 2 от Регламент 2016/679, нейният размер е регламентиран в чл. 83, § 5,буква „д“ от Регламента;

1.7. двете дирекции „ППН“ и „ПАИКД“ поддържат общ регистър за отказ от съдействие със следните реквизити: наименование на АЛД/ОЛД, ЕИК, вид проверка, нарушение, екип осъществил проверката, номер и дата на издаване на АУАН, номер и дата на издаване на НП.

2. Отказ от съдействие при извършване на проверка по документи

2.1. изпращане на писмо (по пощата, с куриер или на официален електронен адрес), с указан срок за предоставяне на информация, документи, становище и др.;

2.2. получаване на известие за доставяне, доказващо, че писмото е получено от АЛД/ОЛД;

2.3. при неизпращане на необходимите документи в указания срок, при възможност се провежда телефонен разговор с АЛД/ОЛД, който се протоколира и/или се изготвя второ писмо с указание за незабавно изпращане на исканите документи;

2.4. при отказ от съдействие и неизпращане на изисканите документи и доказателства, се изготвя протокол за отказ от съдействие, който се завежда в деловодството;

2.5. протоколът за отказ от съдействие следва да съдържа информация за предприетите от служителите действия, с приложени доказателства за тях – уведомителни писма, писма с искане на становища, документи, известия за доставяне, протоколи за проведени с АЛД/ОЛД телефонни разговори и др.;

2.6. протоколът за отказ от съдействие се внася за одобрение и приемане на заседание на КЗЛД с предложение за стартиране на производство по ЗАНН;

2.7. при обжалване се стартира съдебна фаза;

2.8. при необжалвано, връчено и влязло в сила НП, се изпраща писмо за доброволно плащане на наложената санкция;

2.9. когато не се заплати доброволно, се изпраща на НАП за събиране на вземането по реда на ДОПК;

2.10 Решението на КЗЛД може да съдържа и разпоредителни мерки за извършване на проверка на място, съвместно с органите на МВР, с цел установяване на факти по подадения сигнал и предприемане на нужните корективни мерки.

3. Отказ от съдействие при извършване на проверка на място

3.1. когато с действие или бездействие АЛД/ОЛД възпрепятства извършването на проверка на място в проверявания обект или помещенията, където се обработват лични данни:

3.1.1. съставя се протокол със свидетели членовете на проверяващия екип и при възможност и трети лица, в който се описват конкретните факти и обстоятелства – неявяване, недопускане да се съберат доказателства и др.;

3.1.2. стартиране на производство процедурата по ЗАНН със съставяне на АУАН за отказ от съдействие.

XII. НАЛАГАНЕ НА АДМИНИСТРАТИВНИ САНКЦИИ

1. Принципи

1.1. Налагане на „еквивалентни санкции“:

1.1.1. нарушението на Регламент (ЕС) 2016/679 следва да води до налагане на „еквивалентни санкции“;

1.1.2. въпреки че КЗЛД е независим при избора на корективни мерки измежду посочените в чл. 58, § 2 от Регламент (ЕС) 2016/679, следва да се избягва избирането на различни корективни мерки от надзорните органи в сходни случаи, както и налагането на различна по размер санкция при сходни по тежест и обхват нарушения;

1.1.3. същият принцип се прилага, когато тези корективни мерки се налагат под формата на глоби или имуществени санкции.

1.2. Административните наказания „глоба“ или „имуществена санкция“ – „ефективни, пропорционални и възпиращи“:

1.2.1. налаганите от КЗЛД административните наказания „глоба“ или „имуществена санкция“ следва да бъдат „ефективни, пропорционални и възпиращи“;

1.2.2. административните наказания „глоба“ или „имуществена санкция“ следва да отразяват адекватно естеството, тежестта и последиците от нарушението, като всички факти по случая трябва да се оценяват по начин, който е последователен и обективно обоснован;

1.2.3. оценката за това какви мерки са ефективни, пропорционални и възпиращи във всеки отделен случай, също така ще трябва да отразява целта, преследвана с избраната корективна мярка и/или санкция, т.е. възстановяване на спазването на правилата или санкциониране на неправомерно поведение (или и двете);

1.2.4. принципът на „ефективност, пропорционалност и възпиращ“ (чл. 83, § 1 от Регламент (ЕС) 2016/679), се прилага както в случаите от национален мащаб (чл. 55 от Регламент (ЕС) 2016/679), така и в случаите, свързани с трансгранично обработване на лични данни (съгласно определението в чл. 4, § 23 от Регламент (ЕС) 2016/679).

1.3. Оценка „във всеки конкретен случай“:

1.3.1. оценката се прави „във всеки конкретен случай“;

1.3.2. съгласно Регламент (ЕС) 2016/679 се изисква оценяването на всеки случай да се извършва индивидуално. Отправната точка за такава индивидуална оценка е чл. 83, § 2 от Регламент (ЕС) 2016/679;

1.3.3. при нарушение на Регламент (ЕС) 2016/679 следва да се налагат санкции, включително административни наказания „глоба“ или „имуществена санкция“. При леки нарушения или ако глобата, която може да бъде наложена, представлява несъразмерна тежест за физическо лице, вместо глоба може да бъде отсъдено порицание.

1.4. Хармонизиран подход към административните наказания „глоба“ или „имуществена санкция“:

1.4.1. хармонизираният подход към административните наказания „глоба“ или „имуществена санкция“ в областта на защитата на данните изисква активно участие и обмен на информация между надзорните органи;

1.4.2. целта е глобите или имуществените санкции да не се разглеждат като крайна мярка и да не се избягва налагането им, но същевременно и да не се използват по начин, който би обезсилил ефективността им като инструмент.

2. Критерии за оценка в чл. 83, § 2 от Регламент (ЕС) 2016/679

2.1. Естество на нарушението:

2.1.1. дали се касае за непредприети достатъчни мерки за предотвратяване на незаконосъобразно обработване на лични данни;

2.1.2. фишинг атака или друг умишлен противозаконен подход с цел незаконосъобразно обработване на лични данни;

2.1.3. човешка грешка;

2.1.4. други.....

2.2. Тежест на нарушението:

2.2.1. дали нарушението е извършено умишлено или по небрежност:

а) по принцип „умисъл“ включва съзнаване на характеристиките на нарушението и воля за извършването му, докато „неумишлено“ означава, че не е било налице намерение да се извърши нарушението, но въпреки това АЛД/ОЛД не е положил дължимата грижа, както се изисква по закон;

б) като цяло се приема, че умишлените нарушения, при които се демонстрира явно незачитане на законовите разпоредби, са по-тежки от неумишлените нарушения и че поради това при първите е по-вероятно да е основателно налагането на административно наказание „глоба“ или „имуществена санкция“;

в) съответните заключения дали нарушението е извършено умишлено, или по небрежност се правят въз основа на данните за обективните елементи на поведението, събрани от фактите по случая;

г) ако АЛД/ОЛД умишлено или по небрежност наруши няколко разпоредби на настоящия Регламент2016/679 или ЗЗЛД при една и съща операция по обработването или при свързани оператори, общият размер на административната глоба или имуществена санкция не следва да надвишава сумата, определена за най-тежкото нарушение.

2.3. Продължителност на нарушението:

2.3.1. продължителността на нарушението може да е индикация например за:

а) умишлено поведение от страна на администратора;

б) непредприемане на подходящи превантивни мерки;

в) неспособност да се въведат изискваните технически и организационни мерки.

2.3.2. когато се оценяват фактите по случая в светлината на общите критерии, предвидени в чл. 83, § 2 от Регламент (ЕС) 2016/679 може да се реши, че в конкретния случай има по-голяма или съответно по-малка необходимост да се реагира с корективна мярка под формата на глоба или имуществена санкция;

2.3.3. когато бъде наложена глоба или имуществена санкция като единствената или като една от няколко подходящи корективни мерки, се прилага категоризацията от Регламент (ЕС) 2016/679 (чл. 83, §§ 4–6), за да се определи максималната глоба или имуществена санкция, която може да бъде наложена в съответствие с естеството на въпросното нарушение;

2.3.4. „леки нарушения“:

а) могат да представляват нарушение на една или няколко от разпоредбите на Регламент (ЕС) 2016/679, посочени в чл. 83, § 4 или § 5;

б) в резултат на оценката на критериите в чл. 83, § 2 обаче надзорният орган може да счете, че в конкретните обстоятелства по случая нарушението например не създава значителен риск за правата на съответните субекти на данни и не засяга същността на въпросното задължение. В такива случаи глобата или имуществената санкция може (но невинаги) да бъде заменена с порицание.

2.3.5. надзорният орган няма задължение винаги да заменя глоба или имуществена санкция с порицание в случай на леко нарушение („вместо глоба може да бъде отсъдено порицание“), а по-скоро възможност, която може да бъде използвана след извършването на конкретна оценка на всички обстоятелства по случая.

2.4. Несъразмерна тежест на наложената глоба или имуществена санкция:

2.4.1. съображение 148 от Регламент (ЕС) 2016/679 осигурява възможност за замяна на глоба или имуществена санкция с порицание, когато администраторът е физическо или юридическо лице и глобата или имуществената санкция, която може да бъде наложена, би представлявала несъразмерна тежест. Отправната точка за това е, че трябва да се прецени дали се изисква налагането на глоба или имуществена санкция с оглед на обстоятелствата по разглеждания случай;

2.4.2. при преценка, че следва да се наложи глоба или имуществена санкция, трябва също така да се прецени дали тя би представлявала несъразмерна тежест за дадено физическо или юридическо лице;

2.4.3. задължително се прави преценка на администратора относно това дали е микропредприятие, малко или средно предприятиепо смисъла на чл. 3 от Закона за малките и средните предприятия, предвид техните специални потребности и налични ресурси при определяне размера на санкцията и нейната целесъобразност;

2.4.4. в Регламент (ЕС) 2016/679 не се посочват конкретни суми за отделни нарушения, а само таван (максимален размер). Това може да бъде индикация за относително по-ниска степен на тежест при нарушение на задълженията, посочени в чл. 83, § 4, в сравнение с посочените в чл. 83, § 5. Ефективният, пропорционален и възпиращ отговор на нарушение на чл. 83, § 5 обаче ще зависи от обстоятелствата по случая;

2.4.5. нарушенията на Регламент (ЕС) 2016/679, които по своето естество могат да попадат в категорията „до 10 000 000 EUR или до 2 % от общия годишен световен оборот“, както е посочено в чл. 83, § 4 от Регламент (ЕС) 2016/679, при определени обстоятелства могат да бъдат причислени към по-висока категория (20 милиона евро):

а) такъв вероятно би бил случаят, ако тези нарушения вече са били предмет на разпореждане на надзорния орган, което АЛД/ОЛД не е спазил (чл. 83, § 6 от Регламент (ЕС) 2016/679);

б) на практика разпоредбите на националното законодателство могат да окажат въздействие върху тази оценка;

в) редом с естеството на нарушението, „обхватът или целта на съответното обработване, както и броят на засегнатите субекти на данни и степента на причинената им вреда“ също са показателни за тежестта на нарушението;

г) при наличието на няколко отделни нарушения, извършени заедно в рамките на конкретен единичен случай, може да се наложи административни наказания „глоба“ или „имуществена санкция“ на ниво, което е ефективно, пропорционално и възпиращо, като не надхвърля максималния размер за най-тежкото нарушение. Следователно ако бъде установено нарушение на чл. 8 и чл. 12 от Регламент (ЕС) 2016/679, надзорният орган може да наложи корективните мерки, определени в чл. 83, § 5 от Регламент (ЕС) 2016/679, които отговарят на категорията на по-тежкото нарушение, а именно на нарушението на чл. 12 от Регламент (ЕС) 2016/679.

2.5. Брой на засегнатите лица и цел на обработването на лични данни:

2.5.1. следва да се оцени броят на засегнатите субекти на данни, за да се определи дали това е изолиран случай, или показва по-системно нарушение или липса на подходящи практики;

2.5.2. това не означава, че изолираните случаи не следва да подлежат на действия по правоприлагане, тъй като дори един изолиран случай може да засегне множество субекти на данни;

2.5.3. трябва да се оцени целта на обработването на данни:

а) в становището на Работната група по член 29 относно „ограничаването в рамките на целта“ са анализирани двата основни градивни елемента на този принцип в законодателството за защита на данните: конкретизиране на целта и съвместимо използване;

б) когато оценяват целта на обработването в контекста на чл. 83, § 2 от Регламент (ЕС) 2016/679, следва да се проучват степента, в която при обработването се спазват двата основни компонента на този принцип.

2.6. Размер и относителна тежест на настъпилите и/или възможно да настъпят вреди за субектите на данни:

2.6.1. трябва да бъде взета предвид степента на причинените им вреди;

2.6.2. обработването на лични данни може да породи рискове за правата и свободите на лицата, както е посочено в съображение 75 от Регламент (ЕС) 2016/679:

„Рискът за правата и свободите на физическите лица, с различна вероятност и тежест, може да произтича от обработване на лични данни, което би могло да доведе до физически, материални или нематериални вреди, по-специално: когато обработването може да породи дискриминация, кражба на самоличност или измама с фалшива самоличност, финансови загуби, накърняване на репутацията, нарушаване на поверителността на лични данни, защитени от професионална тайна, неразрешено премахване на псевдонимизация, или други значителни икономически или социални неблагоприятни последствия; или когато субектите на данни могат да бъдат лишени от свои права и свободи или от упражняване на контрол върху своите лични данни; когато се обработват лични данни, които разкриват расов или етнически произход, политически възгледи, религиозни или философски убеждения, членство в професионална организация, и обработването на генетични данни, данни за здравословното състояние или данни за сексуалния живот или за присъди и нарушения или свързани с тях мерки за сигурност; когато се оценяват лични аспекти, по-специално анализиране или прогнозиране на аспекти, отнасящи се до представянето на работното място, икономическото положение, здравето, личните предпочитания или интереси, надеждността или поведението, местонахождението или движенията в пространството, с цел създаване или използване на лични профили; когато се обработват лични данни на уязвими лица, по-специално на деца; или когато обработването включва голям обем лични данни и засяга голям брой субекти на данни“.

2.6.3. налагането на глоба или имуществена санкция не зависи от това, дали надзорният орган е в състояние да установи причинно-следствена връзка между нарушението и имуществените вреди (вж. например чл. 83, § 6 от Регламент (ЕС) 2016/679);

2.6.4. примери за обстоятелства, които са показателни за умишлени нарушения, могат да бъдат:

а) неправомерно обработване на данни, разпоредено изрично от висшето ръководство на администратора или в разрез със съветите на длъжностното лице по защита на данните;

б) при незачитане на съществуващи политики, например получаване и обработване на данни относно служителите на конкурентно дружество с цел дискредитирането му на пазара;

в) промяната на лични данни, за да се създаде подвеждащо (положително) впечатление, че дадени цели са постигнати;

г) търговията с лични данни за маркетингови цели, т.е. продажбата на данните като данни, за които е дадено разрешение за обработване от субектите на данни, като не се проверява или се пренебрегва тяхното мнение за това как следва да бъдат използвани техните данни.

2.6.5. други обстоятелства, като например непознаване и неспазване на съществуващите политики, човешка грешка, липса на проверка дали в публикуваната информация има лични данни, липса на своевременно инсталиране на технически актуализации, неприемане на политики (а не просто неприлагането им), могат да са индикация за небрежност.

2.7. Предприети от АЛД/ОЛД действия за смекчаване на последиците от вредите, претърпени от субектите на данни:

2.7.1. когато бъде извършено нарушение и субектът на данни претърпи вреди, отговорната страна трябва да направи всичко възможно, за да ограничи последиците от нарушението за засегнатото лице или лица. Такова отговорно поведение (или липсата му) би трябвало да бъде взето предвид при избора на корективна мярка или мерки, както и при определянето на размера на санкцията, която да бъде наложена в конкретния случай;

2.7.2 въпреки че утежняващите или смекчаващите фактори са особено подходящи за адаптиране на размера на глобата или имуществената санкция с оглед на конкретните обстоятелства по случая, тяхната роля при избора на подходяща корективна мярка не следва да се подценява:

а) в случаите, когато оценката въз основа на други критерии не позволява на надзорния орган категорично да заключи, че е уместно да се наложи административното наказание „глоба“ или „имуществена санкция“ като самостоятелна корективна мярка или в съчетание с други мерки по чл. 58 от Регламент (ЕС) 2016/679, такива утежняващи или смекчаващи обстоятелства могат да помогнат при избора на подходящи мерки, като наклонят везните към мерките, които са по-ефективни, пропорционални и възпиращи в дадения случай;

б) тази разпоредба функционира като оценка на степента на отговорност на АЛД/ОЛД след извършването на нарушението. Тя може да обхване случаи, в които АЛД/ОЛД очевидно не е подходил необмислено/небрежно, и е направил всичко възможно да коригира своите действия, когато е разбрал за нарушението.

2.7.3. може да бъде уместно да се действа с известна степен на гъвкавост спрямо АЛД/ОЛД, които са признали своите нарушения и са поели отговорност да

коригират или ограничат въздействието от своите действия. Това може да включва (макар да не би довело до по-гъвкав подход във всеки отделен случай) примери като:

а) осъществяване на контакт с други АЛД/ОЛД, които може да са участвали в допълнително обработване на данните, например ако част от данните погрешно са били споделени с трети страни;

б) своевременни действия, предприети от АЛД/ОЛД, с цел да не се позволи нарушението да продължи или да се разрасне до степен или етап, на който би имало много по-сериозно въздействие.

2.8. Степен на отговорност на АЛД/ОЛД, като се вземат предвид технически и организационни мерки, въведени от тях в съответствие с чл. 25 и чл. 32 от Регламент (ЕС) 2016/679:

2.8.1. въпросът, на който след това трябва да отговори надзорният орган, е до каква степен АЛД/ОЛД е „отговорил на очакванията“ предвид естеството, целите или обема на обработването с оглед на наложените му задължения съгласно Регламент (ЕС) 2016/679;

2.8.2. при тази оценка следва надлежно да се вземат предвид всички процедури или методи, представляващи „най-добри практики“, когато такива съществуват и се прилагат;

2.8.3. важно е да се вземат предвид стандартите в съответния отрасъл, както и кодексите за поведение в съответната област или професия;

2.8.4. макар че в идеалния случай по принцип следва да се прилагат най-добрите практики, при оценката на степента на отговорност по всеки конкретен случай трябва да се вземат предвид специфичните обстоятелства.

2.9. Предишни нарушения, извършени от АЛД/ОЛД:

2.9.1. извършвал ли е АЛД/ОЛД същото нарушение и преди;

2.9.2. извършвал ли е АЛД/ОЛД нарушение на Регламент (ЕС) 2016/679 и ЗЗЛД по същия начин (например вследствие на недостатъчни знания за съществуващите рутинни практики в организацията или вследствие на неподходяща оценка на риска, липса на своевременен отговор на искания от субекта на данни, необосновано забавяне при отговора на искания и др.).

2.10. Степен на сътрудничество с надзорния орган с цел отстраняване на нарушението и смекчаване на евентуалните неблагоприятни последици от него:

2.10.1. чл. 83, § 2 от Регламент (ЕС) 2016/679 предвижда степента на сътрудничество да може да се разглежда „надлежно“, когато се взема решение дали да

бъде наложено административно наказание „глоба“ или „имуществена санкция“ и се определя нейният размер;

2.10.2. следва да се отчете има ли съответния АЛД/ОЛД длъжностно лице по защита на данните, както и нивото на сътрудничеството с Надзорния орган, което съответно да се отрази върху размера на наложената санкция или нейното редуциране;

2.10.3. следният въпрос представлява пример за случай, при който евентуално би било уместно да се отчете сътрудничеството с надзорния орган:

а) реагирал ли е АЛД/ОЛД по определен начин на исканията на надзорния орган на етапа на разследване на конкретния случай, в резултат на което въздействието върху правата на лицата е било ограничено значително.

2.11. Категории лични данни, засегнати от нарушението:

2.11.1. примери за ключови въпроси, на които надзорният орган може да счете за необходимо да отговори в тази връзка, според случая:

а) свързано ли е нарушението с обработване на специални категории данни по чл. 9 или чл. 10 от Регламент (ЕС) 2016/679;

б) могат ли данните да бъдат идентифицирани пряко или непряко;

в) обработването включва ли данни, разпространението на които би довело до непосредствени вреди/затруднения за лицето (и които попадат извън обхвата на категориите по чл. 9 или чл. 10 от Регламент (ЕС) 2016/679;

г) достъпни ли са данните пряко, без да е налице техническа защита, или са криптирани.

2.12. Уведомяване на надзорния орган за нарушението:

2.12.1. начина, по който нарушението е станало известно на надзорния орган, по-специално дали и до каква степен АЛД/ОЛД е уведомил за нарушението;

2.12.2. съгласно Регламент (ЕС) 2016/679 АЛД е задължен да уведоми надзорния орган за нарушения на сигурността на личните данни. Когато АЛД /ОЛД просто изпълнява това задължение, спазването му не може да се тълкува като смекчаващ фактор;

2.12.3. по подобен начин надзорният орган може да счете, че АЛД/ОЛД, който е действал небрежно, без да уведоми за нарушението, или поне без да уведоми за всички подробности по него, поради неадекватна оценка на степента на нарушението, също заслужава по-сериозна санкция, т.е. това вероятно няма да бъде категоризирано като леко нарушение.

2.13. Налагани мерки, посочени в чл. 58, § 2 от Регламент (ЕС) 2016/679, във връзка със същия предмет на обработването:

2.13.1. спазени ли са предишни налагани мерки на засегнатия АЛД/ОЛД, посочени в чл. 58, § 2 от Регламент (ЕС) 2016/679, във връзка със същия предмет на обработването;

2.13.2. този критерий за оценка цели единствено да напомни на надзорните органи да вземат предвид мерките, които самите те са постановили по-рано за същия АЛД/ОЛД „във връзка със същия предмет на обработването“.

2.14. Придържане към одобрени кодекси на поведение съгласно чл. 40 от Регламент (ЕС) 2016/679 или одобрени механизми за сертифициране съгласно чл. 42 от Регламент (ЕС) 2016/679:

2.14.1. когато АЛД/ОЛД се е придържал към одобрен кодекс на поведение, надзорният орган може да се увери, че самата общност, която отговаря за прилагането на този кодекс, предприема подходящи действия срещу своя член, например чрез схеми за наблюдение и изпълнение на въпросния кодекс на поведение;

2.14.2. следователно надзорният орган може да счете, че тези мерки са достатъчно ефективни, пропорционални или възпиращи в конкретния случай и че не е необходимо да се налагат допълнителни мерки от самия надзорен орган;

2.14.3. независимо от това правомощията на органа за наблюдение не засягат „задачите и правомощията на компетентния надзорен орган“, което означава, че надзорният орган не е задължен да вземе предвид наложените преди това санкции по схемата за саморегулиране.

2.15. Други утежняващи или смекчаващи фактори:

2.15.1 всякакви други утежняващи или смекчаващи фактори, приложими към обстоятелствата по случая, като пряко или косвено реализирани финансови ползи или избегнати загуби вследствие на нарушението;

2.15.2. самата разпоредба съдържа примери за това какви други елементи могат да бъдат взети предвид, когато се определя дали административното наказание „глоба“ или „имуществена санкция“ е подходящо във връзка с нарушение на разпоредбите, посочени в чл. 83, §§ 4–6 от Регламент (ЕС) 2016/679.

3. Комулативно налагане на корективна мярка по чл. 58, § 2 от Регламент (ЕС) 2016/679 и санкция съгласно чл. 83, § 2 от Регламент (ЕС) 2016/679

3.1. нарушителят се санкционира по реда на ЗАНН за допуснато нарушение, като едновременно с това може да се приложи корективна мярка – с конкретни разпореждания за предприемане, с цел недопускане на повторно нарушение или друго подобно, като за издадената корективна мярка и нейното изпълнение следва да уведоми в срок КЗЛД;

3.2. едновременно с Решението по жалба, КЗЛД може да наложи санкция, както и да наложи комулативно корективна мяркапо чл. 58, § 2 от Регламент (ЕС) 2016/679;

3.3. комулативното прилагане на мерките се допуска след преценка смекчаващи и отежняващи обстоятелства и факти, с цел приложените мерки да бъдат ефективни, пропорционални и възпиращи за постигане целите на Регламент (ЕС) 2016/679 и ЗЗЛД по отношение на защитата на физическите лица при обработване на личните им данни.

Забележки:

- за всяка проверка на място, когато съществуват проблемни комуникации или затруднения за осъществяването им, може да се изиска съдействие от органите на МВР – писмено или чрез свързване по телефона със съответният ръководител на местна структура на МВР, въз основа на Споразумение за съдействие във всеки етап на проверката (предварителна подготовка, по документи и на място);
- при констатирането на факти и обстоятелства по време на проверките на място задължително присъстват поне двама от членовете на проверяващия екип;
- в хода на извършване на проверки със заповед на Председателя на КЗЛД може да се промени състав на проверяващия екип като се сменят вече определени или се добавят нови членове на екипа;
- при осъществяване на контролната дейност на КЗЛД, Председателят и членовете на КЗЛД, и членовете на проверяващите екипи спазват Етичния кодекс за поведение на КЗЛД.

Настоящата Инструкция е изготвена на основание чл. 12, ал. 10 от ЗЗЛД и е приета с Решение на КЗЛД от проведено на 29.05.2020 г. на заседание (Протокол № 23 от 29.05.2020 г.), изменена и допълнена с Решение на КЗЛД на заседание, проведено на 24.06.2021 г. (Протокол № 27 от 24.06.2021 г.).