ОБЩИ МЕТОДИЧЕСКИ УКАЗАНИЯ ЗА ПРИЛАГАНЕ НА РЕГЛАМЕНТ (ЕС) 2016/679 НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА ОТ 27 АПРИЛ 2016 ГОДИНА ОТНОСНО ЗАЩИТАТА НА ФИЗИЧЕСКИТЕ ЛИЦА ВЪВ ВРЪЗКА С ОБРАБОТВАНЕТО НА ЛИЧНИ ДАННИ И ОТНОСНО СВОБОДНОТО ДВИЖЕНИЕ НА ТАКИВА ДАННИ И ЗА ОТМЯНА НА ДИРЕКТИВА 95/46/ЕО (ОБЩ РЕГЛАМЕНТ ОТНОСНО ЗАЩИТАТА НА ДАННИТЕ) В ДЪРЖАВНАТА АГЕНЦИЯ ЗА БЕЖАНЦИТЕ ПРИ МИНИСТЕРСКИЯ СЪВЕТ

Преамбюл

Целта на настоящите Общи методически указания е да се предоставят ключови насоки и разяснение във връзка с практическото прилагане на комплексните изисквания на Регламент (ЕС) 2016/679 от страна на прилежащите регионални структури, като се засяга обмена на данни с Държавната агенция за бежанците при Министерския съвет (ДАБ при МС).

Настоящите Методически указания представляват информационен документ и не претендират за изчерпателност.

I. Проучване и анализ на всички процеси по обработване на лични данни в рамките на структурата

1. Първоначално следва да се извърши т.нар. „инвентаризация“ на процесите по обработване, чиято цел е да се идентифицират всички процеси, при които се обработват лични данни. В рамките на структурата следва да се проследят реалните процеси и практики, свързани с обработването на лични данни, в т.ч. като се идентифицират и анализират правомощията/задълженията/ на лицата, обработващи лични данни, начинът на възлагане на обработване на лични данни на лица вътре във ведомствата и извън него, достъпът до тях и начинът на обработване на лични данни.

Обработването на лични данни е всяка операция или съвкупност от операции, извършвана с лични данни или набор от лични данни чрез автоматични или други средства като събиране, записване, организиране, структуриране, съхранение, адаптиране или промяна, извличане, консултиране, употреба, разпространяване или друг начин, по който данните стават достъпни или комбиниране, ограничаване, изтриване или унищожаване.

От своя страна „лични данни“ са всяка информация, свързана с идентифицирано физическо лице или такова, което може да бъде идентифицирано (“субект на данни“), пряко или непряко, по-специално чрез идентификатор като име, идентификационен номер, данни за местонахождение, онлайн идентификатор или по един или повече признаци, специфични за физическата, физиологична, генетичната, психическата, умствената, икономическата, културната или социална идентичност на това физическо лице.

2. След събирането на пълния набор от информация в хода на инвентаризацията, следва да се извърши и последващ анализ относно следното:

2.1 основанията за обработването- дали е във връзка с изпълнение на законово задължение или с оглед изпълнението на задача от обществен интерес или при упражняването на официални правомощия. Основанията за обработване на лични данни са изчерпателно изброени в чл. 6, параграф 1, чл. 9, параграф 2 и чл. 10 от Регламент (ЕС) 2016/679. Всеки процес по обработване на лични данни, който не се извършва на някое от основанията е незаконосъобразен.

2.2 спазването на принципите на обработване на лични данни /законосъобразност, добросъвестност, прозрачност, ограничение на целите, точност, ограничение на съхранението, цялостност и поверителност, отчетност- чл. 5 от Регламент (ЕС) 2016/679/.

2.3 предприетите технически и организационни мерки за защита на личните данни, съгласно чл. 9 от Регламент (ЕС) 2016/679.

2.4 наличие на вътрешни правила, регламентиращи приложението на тези мерки.

2.5 определяне типа на отношенията с трети лица, свързани с обмен на лични данни /администратор-администратор, администратор-обработващ, обработващ-под-обработващ/

2.6 спазването на задължението за реакция при нарушение на сигурността на личните данни.

II. Предприемане на конкретни мерки по привеждане на дейността на ДАБ при МС в съответствие с изискванията на Регламент (ЕС) 2016/679

Основните мерки, свързани със законосъобразното обработване на лични данни, които администраторите и обработващите лични данни следва да предприемат са както следва:

1. Регистри по чл. 30 от Регламент (ЕС) 2016/679

Регистрите, касаят дейностите, за които администраторът отговаря или когато е обработващ-дейности по обработване, извършени от името на администратора. Изключително важно е да се направи преценка кои дейности се обработват от агенцията, в качеството й на обработващ и кои в качеството й на администратор.

Регистърът по чл. 30 от Регламент (ЕС) 2016/679 наподобява регистрите, които са поддържани и от Комисия за защита на личните данни (КЗЛД) и включва както следва:

1.1 име и координати за връзка на администратора, на представителя на администратора и на длъжностното лице по защита на личните данни;

1.2 цели на обработването на лични данни;

1.3 основание за обработване на лични данни /при сключен договор-изпълнение на предмета на договора/;

1.4 описание на категориите субекти на данни и на категориите лични данни;

1.5 категориите получатели, пред които са или ще бъдат разкрити личните данни, включително получателите в трети държави или международни организации;

1.6 предвидените срокове за изтриване на различните категории лични данни /съгласно нормативната уредба и/или установени вътрешни правила/. В случай на невъзможност за фиксиране на конкретни срокове за съхранение на лични данни, следва да се определят критериите, използвани за определяне на срок за съхранение;

1.7 когато е възможно, общо описание на техническите и организационни мерки за сигурност, съгласно чл. 32, параграф 1 от Регламент (ЕС) 2016/679.

Регистрите следва да се поддържат както в електронен формат, така и в писмена форма и да се предоставя достъп до тях на (КЗЛД) при поискване. В този смисъл, следва да се установи механизъм за проследяване на контролната версия на поддържаните регистри, който да гарантира интегритета на съставения документ и да създаде възможност за проследяване на възникващи промени в процесите на обработване на лични данни.

По отношение на процеса видеонаблюдение, осъществяван по силата на договор за охрана, следва да се има предвид, че регистър „Видеонаблюдение“ се поддържа от юридическото лице, извършващо охранителната дейност. В случай на самоохрана, регистърът се води от администратора.

2. Оценка на въздействието върху защитата на лични данни

Съгласно чл. 35 от Регламент (ЕС) 2016/679 относно защитата на лични данни, оценка на въздействието върху защитата на данните се извършва, когато съществува вероятност определен вид обработване и предвид естеството, обхвата, контекста и целите на обработването, да породи риск за правата и свободите на физическите лица.

3.Вътрешни правила за техническите и организационни мерки за осигуряване на адекватно ниво на сигурност на данните

Съгласно чл. 32 от Регламент (ЕС) 2016/679 администраторът на лични данни следва да въведе и приложи подходящи технически и организационни мерки за защита на личните данни.

Вътрешните правила относно техническите и организационни мерки за защита на личните данни целят да определят правила, мерки и процедури необходими за осигуряване на сигурността на данните.

Във Вътрешните правила се описват правата и задълженията на длъжностното лице по защита на личните данни, задълженията на работниците/служителите при обработване на лични данни, извършването на оценка на въздействие и определяне на нива на защита, списък на регистрите, които се водят от Държавна агенция за бежанците при Министерски съвет, отношения с обработващи лични данни, предприети технически и организационни мерки,

действия при произшествия, нарушение на сигурността, упражняване на правата на субектите на данни, категориите получатели, провеждане на периодични обучения, касаещи необходимостта от обработване на лични данни, както и заличаването им.

4. Политика за защита на личните данни

На основание чл. 13 и чл. 14 от Регламент (ЕС) 2016/679 относно защитата на лични данни, субектите на данни имат право да получат от администратора информация относно обработването на техни лични данни. В тази връзка е необходимо администратора на лични данни да изготви такива документи във връзка с дейностите си по обработване на лични данни.

Политиката относно обработването на лични данни на работниците/служителите следва да бъде връчена за преглед от тяхна страна, като е препоръчително полагането на подпис на всеки един от работниците/служителите в края на политиката.

Политиката за защита на личните данни следва да бъде изготвена и в зависимост от категориите субекти, чиито данни се обработват в рамките на ДАБ при МС

Политиката за защита на личните данни съдържа следните основни реквизити:

4.1 данни, идентифициращи администратора и координатите за връзка с него;

4.2 координатите за връзка с длъжностното лице по защита на личните данни;

4.3 категориите субекти на данните, които обхваща;

4.4 категориите лични данни, които се обработват;

4.5 целите на обработването, за което личните данни са предназначени;

4.6 правното основание /всички изчерпателно посочени основания за обработване на лични данни са в чл. 6, чл. 9 и чл. 10 от Регламент (ЕС) 2016/679/;

4.7 предоставяне на лични данни и последици при отказ да се предоставят на съответното ведомство;

4.8 други източници, от които се получават лични данни, като държавни, общински и съдебни органи и др.;

4.9 обработване на информация за субекта на данни от трети лица-обработващи лични данни;

4.10 получателите или категориите получатели на лични данни;

4.11 срокът, за който ще се съхраняват личните данни, съответно критериите за определяне на съответния срок;

4.12 правата на субектите на данни по отношение на личните данни /право на информираност, право на достъп, право на коригиране на данни, право на изтриване, прано на ограничаване на обработването, задължение за уведомяване на субекта на данни, право на преносимост на данните, право на възражение, право на уведомяване при нарушение на информационната сигурност/;

4.13 правото на жалбата до надзорния орган- КЗЛД;

4.14 координати на надзорния орган, а именно КЗЛД;

III. Извършване на видеонаблюдение на обекти на ДАБ при МС

Видеонаблюдението е процес на обработване на лични данни, в резултат на който се извършва запис чрез технически средства за видеонаблюдение. Видеозаписите съдържат лични данни, които спомагат за идентифицирането на конкретно физическо лице.

При извършване на видеонаблюдение на входове и изходи, подходи, общи и други помещения, следва субектите на данни да бъдат информирани чрез поставянето на информационни табели на видно място.

Информационните табели следва да съдържат информация, подобна на тези, която се съдържа в Политиките за защита на личните данни.

IV. Отношения с лица, с които се обменят лични данни

Отношенията най-общо се очертават в три типа: между двама администратори и/или администратори-обработващи, както и между обработващ-подобработващ.

Администратор-физическо или юридическо лице, публичен орган, агенция или друга структура, която сама или съвместно с други определя целите и средствата за обработването на лични данни.

Обработващ-физическо или юридическо лице, публичен орган, агенция или друга структура, която обработва лични данни от името на администратора.

При обмен на данни между/с публични органи и др. подобни, обменът на данни следва да е уреден в нормативен акт. При обмяна на данни с юридическа лица /субекти на частното право/ отношенията следва да се уредят в договор или друг правен акт. В нормативния акт/договора следва да се посочи следното:

1.видове лични данни, които се обработват;

2.субекти, за които се отнасят данните;

3.основание за обработване;

4.срок за обработване;

5.технически и организационни мерки, които се предприемат с оглед гарантиране на сигурност на личните данни;

6.описание на правата и задълженията на двете страни /администратор-администратор; администратор-обработващ/.

Когато обработването се извършва въз основа на договор, отношенията могат да се уредят, посредством анекс/допълнително споразумение към договора /договори за видеонаблюдение, за охрана и тн./.

При провеждането на процедури по реда на Закона за обществените поръчки /ЗОП/ е резонно да се изготвят договори между възложител-изпълнител, в които се взима предвид обработването на лични данни, като се посочи ясно и дали какви процеси по обработване на данни ще бъдат извършени от подизпълнители. В процедурите по реда на ЗОП следва да се уведомят участниците за обработването на лични данни от страна на ДАБ при МС във връзка с провеждането на процедурата, физическите и юридическите лица, участници в процедурата, както и съответната документация.

V. Въвеждане на процедура за уведомяване на надзорния орган /КЗЛД/ и съобщаване на субектите на данни за нарушение на сигурността на личните данни

При нарушение на сигурността на данните администраторът, на основание чл. 33 от Регламент (ЕС) 2016/679, следва да уведоми надзорния орган (КЗЛД) за това нарушение в предвидения 72-часов срок.

При оценка на риска, при който вероятността нарушението на сигурността на личните данни да породи висок риск за правата и свободите на физическите лица, то това обстоятелство следва да бъде съобщено и на субектите на данни /чл. 34 от Регламент (ЕС) 2016/679/. Предвид на това е необходимо и въвеждането на процедура, в която да са описани действията, които ще се предприемат в случай на нарушение на сигурността на данните, основните отговорници за извършването на дейностите при възникване на инцидент, както и сроковете, които следва да се спазват.

VI. Длъжностно лице по защита на личните данни

Съгласно Регламент (ЕС) 2016/679 длъжностното лице по защита на личните данни е задължително за:

1.публичен орган или структура, освен когато става въпрос за съдилища с оглед изпълнение на функциите им;

2.администратори, чиято дейност, поради своето естество, обхват и цели, изискват редовно и мащабно наблюдение на субекти на данни;

3.администратори, чиито основни дейности се състоят в обработване на специални категории данни и на данни, свързани с присъди и нарушения.

Длъжностното лице по защита на личните данни има следните задължения, както следва:

1. да информира и съветва администратора или обработващия лични данни и работниците/служителите, които извършват обработване за техните задължения;

2. да наблюдава спазването на правилата за защита на личните данни и на политиките на администратора или обработващия лични данни по отношение на защитата на личните данни;

3. да предоставя съвети по отношение на оценката на въздействието върху защитата на данните и да наблюдава извършването на оценката;

4. да си сътрудничи с надзорния орган (КЗЛД) и да действа като точка за контакт по въпроси, свързани с обработването /консултация по всякакви въпроси/;

5. да действа като точка за контакт за субектите на данни, касаещи обработването на лични данни, упражняването на правата им съгласно Регламент (ЕС) 2016/679, националното законодателство;

Съгласно Регламент (ЕС) 2016/679 длъжностното лице по защита на личните данни може да бъде член на персонала или на обработващия лични данни. Длъжностното лице по защита на личните данни може да съвместява дейността си с други функции, при условие, че се гарантира отсъствие на конфликт на интереси. Длъжностите, при които може да възникне конфликт на интереси при изпълнение на функциите, вменени на длъжностното лице по защита на личните данни, включват ръководни позиции, както и такива, касаещи целите за обработване на лични данни. Длъжностното лице по защита на личните данни е на пряко подчинение на Председателя на ДАБ при МС.

VII.Спазване на основните принципи, свързани с обработването на лични данни

1."Добросъвестност"-всеки процес по обработване на лични данни следва да съответства на преследваната цел, да не се обработва непропорционален обем от лични данни и да не навлиза прекомерно в личната сфера на субектите на данни.

В рамките на администрацията, добросъвестно е обработването, което държи сметка за предвидените в нормативната уредба данни, които следва да се обработват. Всяко обработване на лични данни, което се отклонява от тези параметри би било недобросъвестно. Недобросъвестно /респ. незаконосъобразно/ би било обработване, което се отклонява от първоначалните цели, за които данните са били събрани. Такова отклонение е допустимо само въз основа на съгласието на субекта или въз основа на законодателството.

Когато обемът от лични данни, необходим за постигане на целта на обработване, не е посочен в нормативен акт, следва лицата, имащи управленски правомощия да упражняват контрол за спазването на принципа на добросъвестност. Лицата, упражняващи управленски правомощия, следва също да контролират дали подчинените им лица спазват указанията за спазване на принципа.

2."Законосъобразност"-същият е обвързан с обработването на лични данни въз основа на конкретно правно основание. За повечето категории лични данни, правните основания са уредени изчерпателно в чл. 6, параграф 1 от Регламент (ЕС) 2016/679. За специалните категории лични данни ("чувствителни данни") е необходимо да е налице някое от условията за обработване по чл. 9, параграф 2 от Регламент (ЕС) 2016/679.

Всеки процес по обработване на лични данни следва да е придружен с конкретна цел за обработването на лични данни и конкретно правно основание.

3."Прозрачност"-предоставянето на информация на лицата по най-леснодостъпната форма. Администраторът на лични данни следва да предоставя и да води комуникация със субектите на данни по ефикасен начин, за да се избегне т.нар. „заливане с информация".

4. „Свеждане на данните до минимум"-ограничаване на обработването на лични данни до необходимото във връзка със целите, за които се обработват.

5. „Точност“-личните данни следва да бъдат поддържани в актуален вид. Предвид на това е необходимо разработването на методика за актуализиране на данните в рамките на процеса на обработване на същите.

6. „Ограничение на съхранението“-установените срокове за съхранение на лични данни следва да се спазват, като съхранението на лични данни за по-дълъг срок не следва да се допуска.

7. „Отчетност“- доказване и документиране на спазването на всички останали принципи относно обработването на лични данни.

Администраторът на лични данни носи отговорност за спазването на изискванията за защита на личните данни и следва да е в състояние да докаже това съответствие. Същият следва да е наясно какви данни се събират и за какви цели, както и да са налични разработени вътрешни механизми, правила и процедури, касаещи спазването на правилата за защита на личните данни.

Основните инструменти за спазване на този принцип са:

7.1 поддържане на регистри на дейностите по обработване на лични данни, на основание чл. 30 от Регламент (ЕС) 2016/679;

7.2 изготвяне на Вътрешни правила за осигуряване на адекватно ниво на защита на личните данни, както и водене на списък на всички релевантни документи, относими във връзка с приложението им;

7.3 изготвяне на Вътрешни правила за документооборота;

7.4 разработване на политики за защита на личните данни- това от своя страна осигурява обективиране на факта, че субектите на лични данни са уведомени относно личните данни, които се събират за тях, целите и основанията за тяхното обработване, сроковете за съхранение и правата на субектите /чл. 13 и чл. 14 от Регламент (ЕС) 2016/679/;

7.5 разработване на процедура за уведомяване на надзорния орган (КЗЛД) и за съобщаване на субектите на данни, в случай на нарушение на сигурността на личните данни;

7.6 уреждане на отношенията с лица, с които се обменят лични данни- между двама администратори и/или администратори-обработващи, както и между обработващ-подобработващ;

7.7 назначаване на Длъжностно лице по защита на личните данни;

7.8 установяване на срокове за съхранение на документи, съдържащи лични данни, както на хартиен, така и на електронен носител;

7.9 процедура за изтриване/унищожаване на носители на лични данни /включително копия или работни екземпляри на документи, за които няма установени срокове и правила за съхранение/;

7.10 процедури за коригиране на неточни данни;

7.11 процедура за архивиране и съхранение на хартиени и електронни документи /за електронните писма е необходимо утвърждаването на Вътрешни правила/;

7.12 при извършване на видеонаблюдение-разработване на детайлни информационни табели, които включват информация за правата на субектите на данни;

7.13 извършване на оценка на въздействието при наличие на риск за правата и свободите на физическите лица.

Със цел гаранция за правата и свободите на физическите лица във връзка с обработването на личните им данни, следва да се разработят и утвърдят Вътрешни правила за разглеждане на питания от физически лица, както и към кого могат да се обърнат, сроковете за разглеждането им /съгласно чл. 12 от Регламент (ЕС) 2016/679/.

VIII. Съгласие за обработване на лични данни

Съгласието е правно основание за обработване на лични данни, съгласно чл. 6, параграф 1 от Регламент (ЕС) 2016/679. При необходимост от обработване на лични данни, основаващо

се на съгласие, същото следва да е съобразено с условията й съгласно чл. 7 и чл. 8 от Регламент (ЕС) 2016/679.

IX. Обработване на лични данни при проекти

Препоръчително е правилата относно създаването на регистри и политики за защита на личните данни да се предприемат спрямо основните процеси по обработване на лични данни в периода на проекта.

В случай, че ДАБ при МС е в партньорство с други организации/институции отношенията помежду им следва да се характеризират от типа на съвместни администратори на данни. Съгласно чл. 26 от Регламент /ЕС/ 2016/679 съвместните администратори, на основание чл. 13 и чл. 14, следва да определят отговорностите си за изпълнение на задълженията /упражняването на правата на субекта на данни и съответните им задължения за предоставяне на информация/.

X. Образци на документи, използвани в ДАБ при МС

Във всички образци на декларации, заявления, искания, протоколи и други документи /електронни и на хартия/ на ДАБ при МС, следва да се обозначи дали предоставянето на съответните данни е задължително или договорно изискване или е изцяло доброволно, както и последиците от отказ за предоставяне на данни. При определяне на образци на документи преценката следва да се основава на принципите за добросъвестност, пропорционалност, свеждане на данните до минимум.